

21世纪高等职业教育计算机系列规划教材

物联网工程基础

胡国胜　肖　佳　主　编

方龙雄　束遵国　李天宝　副主编

配备课件

電子工業出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn



21世纪高等职业教育计算机系列规划教材

软件开发

C语言程序设计（徐受蓉、袁可可）
基于ASP.NET的Web应用开发技术实用教程（方玉燕）
Visual C# 2005程序设计项目教程（聂品、黄伟）
Visual Basic程序设计项目教程（刘自昆、李怡平）
JSP网络应用系统开发教程（郭红）
JSP动态网站开发项目教程（徐婉珍）
Java软件开发基础（姚骏屏、张红实）
基于Java技术的Web应用开发（孙璐）
Java程序设计教程（刘青迎）
Java Web应用软件开发（张红实、何桂兰）
Java面向对象应用软件开发（姚骏屏、汪卫星）
Java EE 框架开发技术与设计教程（植挺生）
Java EE 项目应用开发（基于Struts 2，Spring，Hibernate）（刘勇军、王电钢）
基于Struts、Hibernate、Spring架构的Web应用开发（范新灿）
软件测试技术基础（基于工作过程）（魏琴、梅佳）
Android程序设计实用教程（向守超、姚骏屏）
Android应用开发基础教程（曾文权、何拥军）

数据库

SQL Server 2005数据库应用教程（刘勇军、蒋文君）
数据库应用技术项目教程（基于SQL Server 2008）（罗耀军、李湘林）
Oracle 11g数据库项目应用开发（李强）
基于Oracle的Web应用项目开发（朱亚兴、朱旭刚）
SQL语言与关系数据库（黄河、王贤志）
Visual Studio 2010（C#）Windows数据库项目开发（曾建华）

图形图像 / 多媒体

中文版Photoshop CS4平面设计实训案例教程（含DVD1张）（覃俊、雷波）
Photoshop CS4 基础与项目实训教程（赵荣、胡昌杰）
Photoshop CS4 实例教程（蒋斌、罗坚）
平面图像处理应用实例教程（Photoshop CS5+Illustrator CS5）（于宗琴）
Flash CS5 平面动画设计与制作案例教程（田启明）
(2009年国家级精品课程配套教材)
多媒体技术与应用（青巧、黄春华）
影视动画后期制作（含DVD光盘1张）（殷均平、孔素然）
产品包装设计案例教程（王永琦、黄毅英）

网络技术与应用

管理信息系统分析与设计项目教程（于小川、韦智勇）
基于工作过程的商务网站建设—网页制作（黄颖、蒲茜）
Dreamweaver CS4动态网页制作实用教程（罗保山、吴煜煌）
Internet应用（杨莉）
网络规划与设计（李贺华）
网络工程（陈国浪）
局域网组建与交换技术项目教程（陈敏）
广域网架构与路由技术项目教程（陈敏）
组网技术与网络管理（施吉鸣）
网络组建与维护（陈晴）
构建中小型企业网络（谭亮、何绍华）
网络综合布线设计与施工技术（梁裕）
安全网络构建（沈才梁）
网络服务的配置与管理项目实践教程
——基于Windows Server 2008平台（齐跃斗）
网络数据库项目教程
——基于SQL Server 2008（方风波、彭岚）
信息安全基础（胡国胜、张迎春）
信息安全技术与实施（武春岭）
信息安全产品配置与应用（武春岭）

物联网应用技术

物联网工程基础（胡国胜、肖佳）

计算机基础

计算机文化基础教程（第3版）（杨殿生、肖力）
计算机文化基础实训教程（第3版）（徐小平、杨海军）
计算机应用基础（第2版）（郝建春）
计算机应用基础实训指导（第2版）（郝建春）
计算机文化基础（第2版）（梁丹、傅丽霞）
计算机文化基础实训指导（第2版）（梁丹、臧柏齐）
计算机应用基础（肖甘、邱绪桃、李鹏）
计算机应用基础实训指导（肖甘）
计算机应用基础——“教•学•做”一体化（文其知、潘
计算机应用基础（胡国胜）
计算机应用基础实训指导（胡国胜）

操作系统

Windows Server 2008系统管理与维护项目教程（成春华
Linux操作系统应用技术（周志敏）
Linux服务与安全管理（张迎春、胡国胜）

计算机硬件

单片机实践与应用（罗学恒）
计算机组装与维护教程（吕佩徽）

计算机辅助设计

Protel DXP 2004 原理图与电路板设计实用教程（郑梦泽

安全防范技术

现代安防技术设计与实施（陈晴、邓忠伟）
安防系统维护与设备维修（全彩）（温怀疆）

ISBN 978-7-121-20695-5



策划编辑：徐建军
责任编辑：徐建军
封面设计：一克米工作室

定价：32.00元

21世纪高等职业教育计算机系列规划教材

物联网工程基础

胡国胜　肖　佳　主　编

方龙雄　柬遵国　李天宝　副主编

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书系统介绍国内外物联网的发展历程、物联网系统组成、物联网技术的基础理论、实际应用案例和最新的前沿技术。

全书共分为6章，分别介绍物联网在智能农业、智能控制、智能安防、智能超市和智能交通等领域的运用案例，帮助学生全面掌握物联网应用系统方案设计。本着科学性、理论性和实践性相结合的原则，重点剖析RFID技术、无线传感网络技术和物联网无线通信技术等关键技术，并配备大量的实验实训项目帮助学生对物联网技术的理解和掌握。最后从工程角度分析了物联网感知层的安全问题。

本书可作为高职高专物联网相关专业的教材，也可作为企业员工培训、自学的参考书和其他培训用书。

图书在版编目（CIP）数据

物联网工程基础/胡国胜，肖佳主编. —北京：电子工业出版社，2013.7
（21世纪高等职业教育计算机系列规划教材）
ISBN 978-7-121-20695-5

Ⅰ. ①物… Ⅱ. ①胡… ②肖… Ⅲ. ①互联网络－应用－高等职业教育－教材②智能技术－应用－高等职业教育－教材 Ⅳ. ①TP393.4②TP18

中国版本图书馆CIP数据核字（2013）第128775号

策划编辑：徐建军（xujj@phei.com.cn）
责任编辑：徐建军　　特约编辑：俞凌娣
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　　　　北京市海淀区万寿路173信箱　邮编 100036
开　　本：787×1 092　1/16　印张：15.25　字数：390.4千字
印　　次：2013年7月第1次印刷
印　　数：3 000册　定价：32.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着计算机技术、通信技术、微电子技术的发展，特别是 2008 年金融危机的影响，物联网被视为拯救世界经济的“灵丹妙药”。物联网产业已成为我国“十二五”战略性产业，为产业结构的调整提供了千载难逢的机遇，预计到 2020 年，物联网产业将成为国家支柱产业。

物联网快速影响、改善着人们的生活环境和质量，也改变着商业业态。物联网人才需求呈几何级数的增长。高职院校如何培养适合物联网产业发展的高端技术技能型人才是需要认真思考的问题。物联网已被列为国家战略性产业，行业急需大量物联网人才。出版适合高职学生培养的物联网教材是当务之急。

物联网由三层组成：感知层、传输层和应用层。对于高职学生而言，应轻视物联网技术，重视物联网工程和物联网系统集成、维护。学生在完成学业后适合从事感知层（主要涉及 RFID、传感器、安防设备）的安装与调试、传输层的网络施工和通信设备安装维护以及应用层的系统集成等相关岗位。因此，本书摒弃了目前市场上物联网教材的学科体系结构，结合高职学生基础、就业目标和学习目标，遵循高职学生的学习习惯和认知规律。首先对物联网基础知识作一简单介绍，让学生了解物联网发展过程和历史必然。然后，传授学生物联网感知终端（RFID、Sensor）、物联网网络通信技术等基础知识，掌握物联网相关技术的简单应用。在此基础上，学生容易理解物联网的应用和分析案例。最后介绍物联网安全，重点放在物联网工程感知终端安装和维护等安全方面。

全书共分为 6 章，在编写过程中，充分体现项目引领、任务驱动和“教学做”一体的理念，符合高职学生的学习需要，并配备练习题以培养学生的学习能力、发现和解决问题的能力。

本书由上海电子信息职业技术学院组织编写，胡国胜、肖佳担任主编，方龙雄、束遵国、李天宝担任副主编。其中胡国胜参与第 1～6 章的编写，吴俊、李天宝参与第 2 章的编写，束遵国、张东参与第 3、4 章的编写，肖佳、周巧婷参与第 1、5 章的编写，方龙雄、范晓燕参与第 6 章的编写，鲁家皓参与制图，最后由胡国胜统稿并审校。

本书为区别于传统的以理论教学为主的研究型教材，避免空洞枯燥，配备大量案例、图片和练习，并建立了大量物联网视频资料库，加强学生应用能力培养，帮助学生系统地学习物联网技术与方法，掌握基本理论和实践，培养学生运用物联网技术分析和解决实际问题的方法。

本书得到国家骨干院校建设项目、上海市教育科研项目资助，同时得到上海张江 RFID 应用测试公共服务平台、上海企想信息技术有限公司和上海海鼎信息工程股份有限公司的大力支持，在此，一并致以衷心的感谢！

为了方便教师教学，本书配有电子教学课件，请有此需要的教师登录华信教育资源网（www.hxedu.com.cn）免费注册后进行下载。如有问题，可在网站留言板留言或发邮件到 hxedu@phei.com.cn。

由于水平和时间所限，疏漏和错误之处在所难免，敬请广大读者批评指正。

编　者

目 录

第 1 章　物联网简述……（1）
1.1　物联网与生活……（2）
1.1.1　政府引导……（2）
1.1.2　现实应用……（6）
1.2　物联网概述……（11）
1.2.1　物联网与相关术语……（11）
1.2.2　互联网、物联网与物连网……（13）
1.2.3　物联网发展史……（14）
1.3　物联网的关键技术……（14）
1.4　物联网工程的基本架构……（15）
1.5　物联网发展现状……（16）
1.5.1　国外发展情况……（16）
1.5.2　国内发展情况……（19）
1.6　物联网工程面临的问题……（20）
1.6.1　技术问题……（20）
1.6.2　标准问题……（21）
1.6.3　商业模式完善问题……（22）
1.7　练习题……（22）
第 2 章　物联网 RFID 技术……（25）
2.1　自动识别技术……（27）
2.1.1　光符号识别技术……（27）
2.1.2　语音识别技术……（27）
2.1.3　生物识别技术……（28）
2.1.4　IC 卡技术……（30）
2.1.5　射频识别技术……（31）
2.2　RFID 技术……（32）
2.2.1　RFID 发展过程……（32）
2.2.2　RFID 技术标准现状……（34）
2.2.3　RFID 系统组成与工作原理……（36）
2.2.4　阅读器到 RFID 标签的能量传输……（44）
2.2.5　电子产品编码（EPC）技术……（46）
2.3　实训……（51）
2.3.1　实训一：实验箱安装与连接……（51）

2.3.2 实训二：超高频读写器的基本认知 …… (54)
2.3.3 实训三：Gen2 协议下标签读写 …… (57)
2.3.4 实训四：高频读写器的基本认知 …… (60)
2.3.5 实训五：低频读写器的基本认知 …… (63)
2.4 练习题 …… (64)
第 3 章 物联网传感器技术 …… (70)
3.1 传感器技术 …… (71)
3.1.1 什么是传感器 …… (71)
3.1.2 传感器简史 …… (72)
3.1.3 传感器分类 …… (73)
3.1.4 传感器特性 …… (74)
3.1.5 选用原则 …… (75)
3.1.6 大规模长时间部署传感器的设计需求 …… (76)
3.2 ZigBee 协议 …… (77)
3.2.1 ZigBee 基础知识 …… (77)
3.2.2 PC 端数据访问接口协议 …… (79)
3.3 实训 …… (81)
3.3.1 实训一：组建星型 ZigBee 网络 …… (81)
3.3.2 实训二：ZigBee 模块基础信息读取 …… (83)
3.3.3 实训三：ZigBee 基础控制 …… (89)
3.3.4 实训四：ZigBee 传感数据采集 …… (95)
3.4 练习题 …… (106)
第 4 章 物联网无线通信技术 …… (109)
4.1 互联网简述 …… (110)
4.1.1 互联网基本组件 …… (110)
4.1.2 从互联网到物联网 …… (116)
4.2 无线宽带网络 …… (117)
4.2.1 无线网络基本元素 …… (117)
4.2.2 无线网络分类 …… (119)
4.2.3 无线物联世界 …… (121)
4.3 无线低速网络及其协议 …… (122)
4.4 实训 …… (126)
4.4.1 实训一：无线通信路由配置 …… (126)
4.4.2 实训二：建立 WiFi 无线宽带网络 …… (130)
4.4.3 实训三：蓝牙无线传感数据采集与控制 …… (133)
4.4.4 实训四：WiFi 无线传感数据采集与控制 …… (140)
4.4.5 实训五：GPRS 无线传感数据采集与控制 …… (145)
4.5 练习题 …… (150)

第 5 章 物联网工程应用 (152)
5.1 物联网在零售领域的应用 (153)
5.1.1 物联网与商品零售概述 (153)
5.1.2 物联网零售应用 (153)
5.1.3 “未来商店”实例 (156)
5.2 物联网在安防领域的应用 (162)
5.2.1 安全防范自动化 (162)
5.2.2 门禁管理子系统解决方案 (164)
5.2.3 上海浦东国际机场防入侵物联网系统 (165)
5.3 物联网在通信领域的应用 (166)
5.3.1 移动支付 (167)
5.3.2 基于短信的网上购物移动支付解决方案 (168)
5.3.3 世博“手机票” (169)
5.4 物联网在智能交通领域的应用 (171)
5.4.1 物联网智能交通概述 (171)
5.4.2 ETC 收费系统简介 (172)
5.4.3 基于 RFID 的 ETC 解决方案 (174)
5.5 物联网在智能家居领域的应用 (176)
5.5.1 智能家居概述 (176)
5.5.2 智能家居现状 (176)
5.5.3 智能家居系统解决方案 (177)
5.6 物联网在智慧农业领域的应用 (179)
5.6.1 智慧农业现状和趋势 (179)
5.6.2 智慧农业典型应用 (180)
5.7 物联网在食品药品追溯领域的应用 (182)
5.7.1 物联网食品药品安全监管追溯系统 (182)
5.7.2 物联网在药店防伪中的应用 (182)
5.8 练习题 (184)
第 6 章 物联网工程安全 (185)
6.1 物联网工程安全目标 (186)
6.1.1 安全目标 (186)
6.1.2 安全威胁 (186)
6.1.3 安全体系 (187)
6.2 RFID 系统安全 (187)
6.2.1 RFID 物理安全 (188)
6.2.2 RFID 通信安全 (188)
6.2.3 RFID 信息安全 (189)
6.3 无线传感器网络安全 (191)

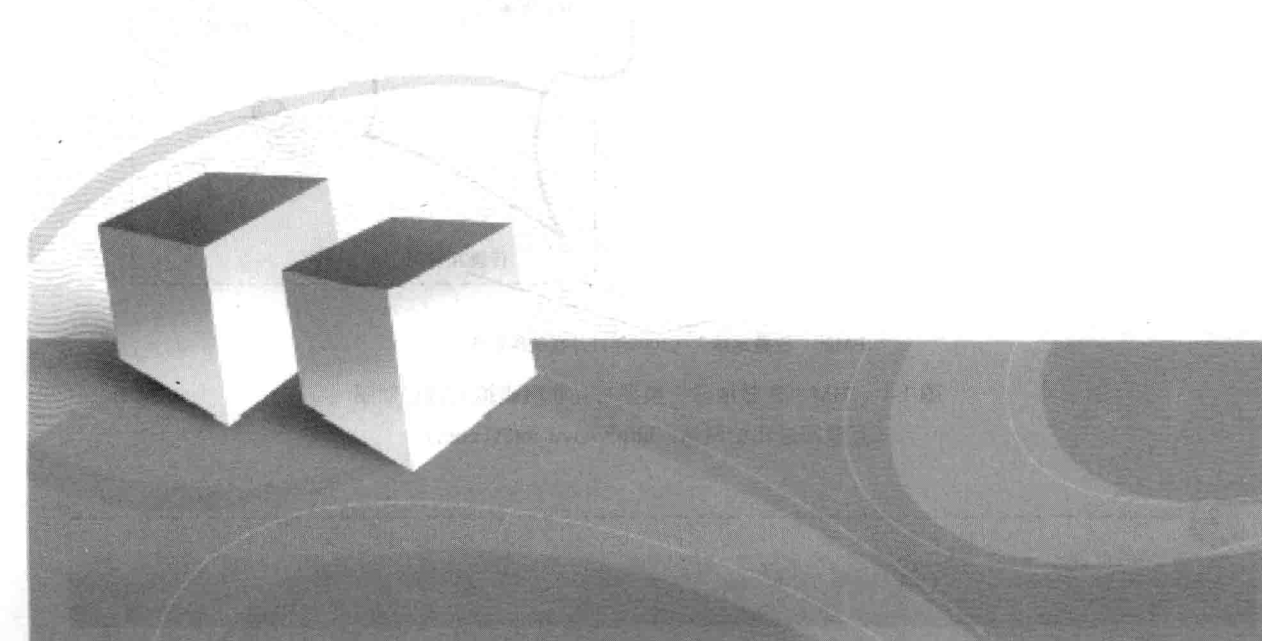
6.4 物联网传输层的安全……（194）
6.5 实训……（196）
6.5.1 实训一：简易防火墙配置……（196）
6.5.2 实训二：VPN 实现……（206）
6.6 练习题……（215）
附录 A DS18B20 温度传感器介绍……（216）
附录 B CH-GWB301 蓝牙/WiFi/GPRS 节点参考指令……（220）
参考文献……（233）

第1章

物联网简述

历史经验表明，根据经济长波理论，每次在大的经济危机发生之后，总会伴随着新技术、新产业和新的经济增长点的诞生，引领和支撑经济的复苏、发展，从而带动社会走出危机的泥潭，进入上升周期。1857年的世界经济危机，引发了以电气革命为标志的第二次技术革命；1929年的世界经济危机，引发了战后以电子、航空航天和核能等技术突破为标志的第三次技术革命；在20世纪末，一系列新兴市场（特别是东南亚）遭受金融危机的打击后，诞生了互联网这一新兴行业。而起源于2008年延续至今的金融海啸重创全球经济，欧美经济面临第二次探底。为此，在人们热切关注新能源行业发展时，在通信、互联网、射频识别等新技术的推动下，一种能够实现人与人、人与机器、人与物乃至物与物之间直接沟通的全新网络构架——物联网（The Internet of Things，IOT）正日渐清晰。

尽管仍有一些学术界或者技术精英对这种说法莫衷一是，但不可否认的是，包括美国、德国在内的先进国家正在试图通过“物联网”走出经济的泥潭，并且开发了相关技术标准和行业标准，逐渐形成垄断态势。我国政府非常重视物联网相关产业的发展，2010年，教育部一次性批准30所本科院校开设物联网专业。



1.1 物联网与生活

1.1.1 政府引导

近来，“物联网”已成为备受推崇的热点词汇，从一般性的网站、电视、广播、报刊，到机上读物、广告宣传，以及技术论坛、行业评估、物联网概念股等，无不在热议“物联网”。在这场科技革命、信息革命的演进过程中，美国前副总统阿尔·戈尔（Al Gore）提出的“数字地球”（Digital Earth）可以让人类随时随地遨游全球；2008 年 11 月，IBM 董事长兼 CEO 彭明盛在纽约召开的外国关系理事会上，正式提出“智慧地球”（Smart Planet），2009 年 1 月，“智慧地球”成为美国国家战略的一部分（“智慧地球”与 2007 年提出的互联网虚拟大脑很相似，如图 1-1 所示）；美国总统奥巴马将物联网与绿色能源并列，认为这两大战略能够带来长短兼顾的良好效益；中国前总理温家宝提出了建立“感知中国”中心工作，物联网建设被悄然上升到国家战略的层面。

互联网虚拟大脑（2007年12月在中国提出）

互联网虚拟大脑的神经系统 | 传统互联网

音频采集器、音频采集器、视频采集器、视频采集器、空气传感器、水系传感器、土壤传感器、办公设备、家用设备、生产设备

虚拟听觉系统、虚拟视觉系统、虚拟感觉系统、虚拟运动系统

1 信息处理中心服务器；2 虚拟神经元

台式机、笔记本、台式机、手机、人

物联网 | 传统互联网

IBM的“智慧地球”（2008年11月在美国提出）

图 1-1　IBM“智慧地球”模型与互联网虚拟大脑相似图

（互联网进化论网站：http://www.intevl.com）



1. 戈尔：数字地球

1998 年 1 月 31 日美国前副总统戈尔在加利福尼亚科学中心，作了题为《数字地球：展望 21 世纪我们这颗行星（Digital Earth: 21st century our planet）》的长篇演讲。他在演讲中，首次提到并系统阐述了“数字地球”这个新概念，其构想如图 1-2 所示。这个概念提出的前提是，技术创新的新浪潮使我们能够大量地获得、存储、处理和显示关于我们行星的各种环境和文化现象的信息。如果大量的信息构成了“地理坐标系”，它将涉及地球表面的每一个特定的地方。有了这个数字化的“地理坐标系”信息源，人类就可以淘汰现在的人—机对话方式，即利用 Macintosh 和 Windows 操作系统提供的桌面图形方式，跨入多种分辨率、三维的表达方式，使人类能嵌入巨大数量的地理坐标系数据。

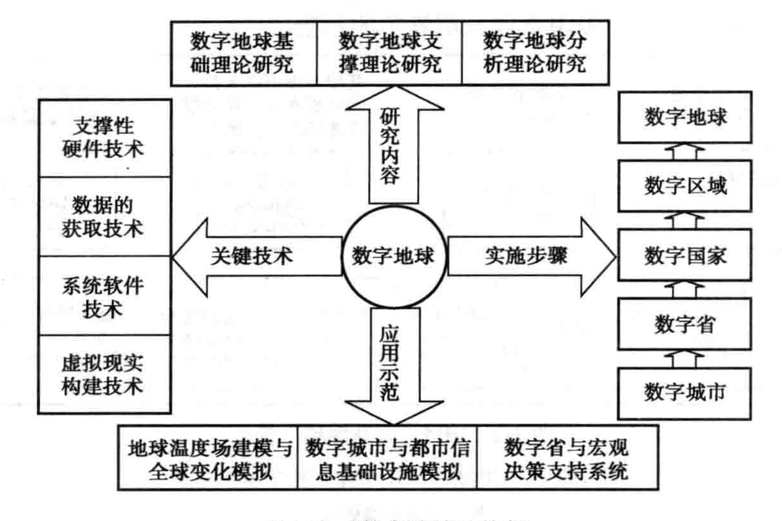


图 1-2 “数字地球”构想

戈尔认为高科技的发展使人类拥有了前所未有的捕捉、收集、处理和展示信息的手段，但大量的数据并没有得到充分处理，更没有得到充分的使用。例如，一颗地球卫星每两周即可发回地球的完整照片，这种卫星已经运行了 20 年，所收集的信息可谓浩如烟海，但只是储存在数据库里，与绝大多数人的日常生活无关。

要利用这么巨大的信息量为人类服务，必须开发新的信息展示技术。人脑处理信息的“技术”具有速率低而分辨率高的特点，一般人难以在短时间内记住 7 组以上的数据，但是由几十亿个信息单元组成的图像，如一处风景、一张名人相片，人们却可以过目不忘。由此，戈尔提出，“我们需要一个‘数字地球’，这是一个高分辨率三维空间的数据星球，与地球有关的庞大数据可以存储在里面”，人们借助头戴显示器、特制的数据手套等高分辨率展示工具，就可以在全球自由遨游，不受时间和空间的限制，可以谈笑间“飞”到万里之外或千年之前，寻访南极的一座冰峰或会晤埃及的某位法老。

2. 奥巴马：智慧地球

20 世纪末，克林顿政府提出“信息高速公路”的国家振兴战略，大力发展互联网，推动了

全球信息产业的革命，美国经济受惠于这一战略的远见卓识，在 20 世纪 90 年代中后期享受了历史上罕见的长期繁荣，使美国的霸主地位继续稳固。

21 世纪初，奥巴马总统面对财政困难、失业率居高不下、房价继续下探、支持率连创新低的危局，正在苦苦求索。奥巴马的振兴战略方向在哪里？种种迹象表明："智慧地球"发展战略将成为主导。

2008 年，IBM 公司提出的"智慧地球"发展战略（见图 1-3），受到美国政府的高度重视。"智慧地球"的核心是：无处不在的智能对象，被无处不达的网络与人连接在一起，再被无所不能的超级计算机调度和控制。与这一战略相关的前所未有的"智慧"的基础设施，为创新提供了无穷无尽的空间，其应用领域如图 1-4 所示。作为新一波信息技术革命，其对于人类文明的影响之深远，将远远超过互联网。预期其中投资于新一代智慧型基础设施建设项目，能够有力地刺激经济复苏，而且能为美国奠定长期繁荣的基础。

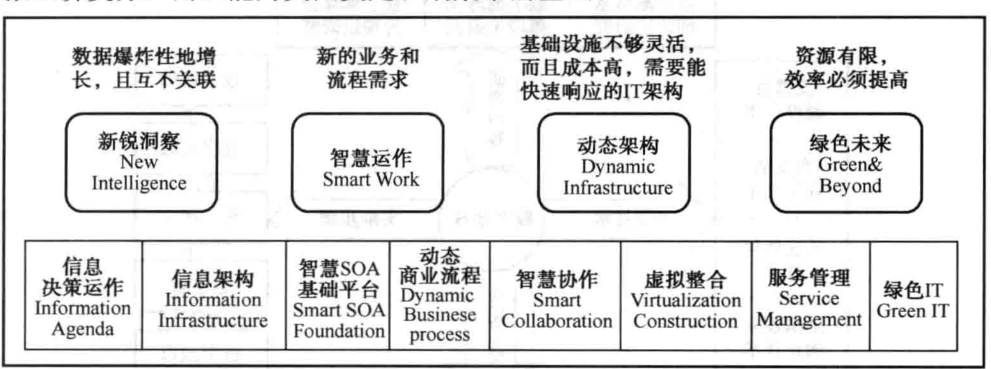


图 1-3 IBM"智慧地球"构思

（IBM-智慧的地球-中国：http://www.ibm.com）



图 1-4 "智慧地球"应用领域

（IBM-智慧地球-中国：http://www.ibm.com）



这一前景，毫无疑问引起了奥巴马团队的兴趣。既然 1993 年的克林顿能够利用互联网革命把美国带出当时的经济低谷，并实现空前的经济繁荣，那么 2009 年的奥巴马或许也可以利用“智慧地球”重现这一幕。“智慧地球”可能上升为美国的国家战略。

3. 温家宝：感知中国

2009 年 8 月 7 日，时任国务院总理温家宝在无锡考察时提出了“感知中国”（Sensing China）战略。

2009 年 11 月 3 日，温家宝在《让科技引领中国可持续发展》讲话中有这样的描述：信息网络产业是世界经济复苏的重要驱动力。全球互联网正在向下一代升级，传感网和物联网方兴未艾。“智慧地球”简单来说就是物联网与互联网的结合，就是传感网在基础设施和服务领域的广泛应用。我在无锡考察时参观了中国科学院微系统所无锡传感网工程中心，很高兴看到一批年轻人正在从事传感网的研究。我相信他们一定能够创造出“感知中国”，在传感世界中拥有中国人自己的一席之地。我们要着力突破传感网、物联网的关键技术，及早部署后 IP 时代相关技术研发，使信息网络产业成为推动产业升级、迈向信息社会的“发动机”。

2010 年 3 月 5 日，温家宝在十一届全国人大三次会议上作政府工作报告时指出：转变经济发展方式刻不容缓。要大力推动经济进入创新驱动、内生增长的发展轨道。温家宝指出，大力培育战略性新兴产业。国际金融危机正在催生新的科技革命和产业革命。发展战略性新兴产业，抢占经济科技制高点，决定国家的未来，必须抓住机遇，明确重点，有所作为。要大力发展新能源、新材料、节能环保、生物医药、信息网络和高端制造产业。积极推进新能源汽车、“三网”融合取得实质性进展，加快物联网的研发应用。加大对战略性新兴产业的投入和政策支持。

此后各级政府出台政策、各高校院所研发技术、标准化进展、设立重大专项等。这一年，中国已有 28 个省市将物联网作为新兴产业发展重点之一；这一年，5 亿元首批物联网专项基金启动以后，国内共有 600 多家企业陆续进行了该基金项目的申报工作，A 股多家上市公司均获得该资金的支持。

2012 年 2 月 14 日，工信部发布《“十二五”物联网发展规划》，多层面的政策投入成为推动现阶段中国物联网产业发展的最强动力。图 1-5 所示为各省市的物联网发展规划。

4. 工业和信息化部四措施推动物联网产业发展

我国物联网总体还处于起步阶段，为推进物联网产业发展，我国将采取四大措施支持电信运营企业开展物联网技术创新与应用。这些措施包括：

一是突破物联网关键核心技术，实现科技创新。同时结合物联网特点，在突破关键共性技术时，研发和推广应用技术，加强行业和领域物联网技术解决方案的研发和公共服务平台建设，以应用技术为支撑突破应用创新。

二是制定我国物联网发展规划，全面布局。重点发展高端传感器、微电子机械系统（Micro-Electro-Mechanical Systems，MEMS）、智能传感器和传感器网节点、传感器网关；超高频射频识别（Radio Frequency Identification，RFID）、有源 RFID 和 RFID 中间产业等，重点发展物联网相关终端和设备以及软件和信息服务。

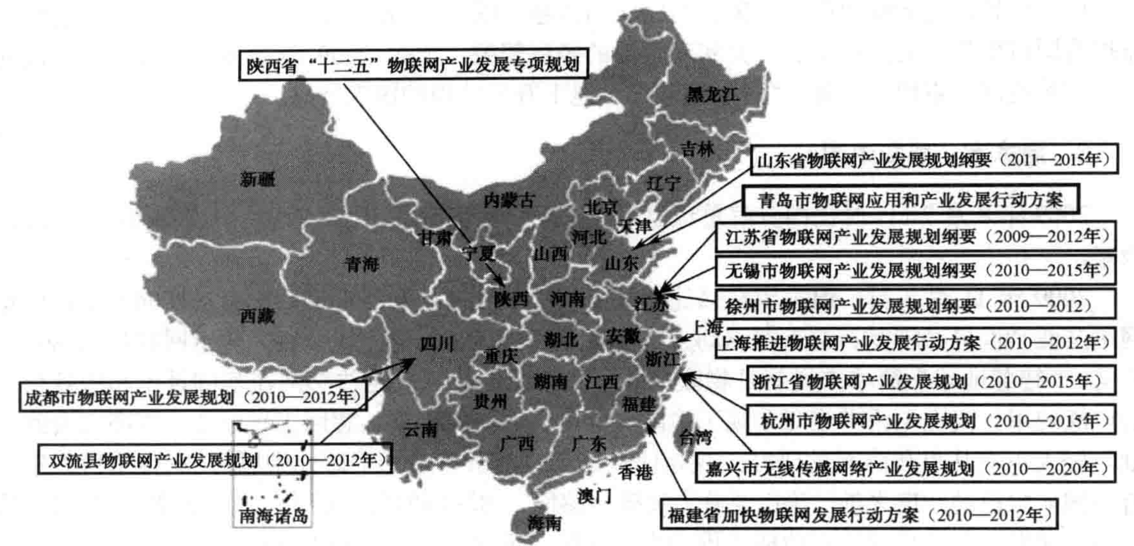


图 1-5　中国部分省市物联网产业发展规划

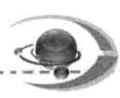
三是推动典型物联网应用示范，带动发展。通过应用引导和技术研发的互动式的发展，带动物联网的产业发展。重点建设传感网在公众服务与重点行业的典型应用示范工程，确立以应用带动产业的发展模式，消除制约传感网规模发展的瓶颈。深度开发物联网采集来的信息资源，提升物联网的应用过程中产业链的整体价值。

四是加强物联网国际国内标准，保障发展。做好顶层设计，满足产业需要，形成技术创新、标准和知识产权协调互动机制。面向重点业务应用，加强关键技术的研究，建设标准验证、测试和仿真等标准服务平台，加快关键标准的制定、实施和应用。积极参与国际标准制定，整合国内研究力量形成合力，推动国内自主创新研究成果推向国际。

1.1.2　现实应用

物联网用途广泛，遍及智能交通、环境保护、政府工作、公共安全、平安家居、智能消防、工业监控、老人护理、个人健康等多个领域。在生活中的应用举不胜举。

- 健康监控。人身上可以安装不同的传感器，对人的健康参数，如体温、血压、心电图和血氧监测等进行监控，保健中心通过手机，提醒您去医院检查身体，如图 1-6 所示。
- 智能耕作。2002 年，Intel 公司率先在俄勒冈建立了世界上第一个无线葡萄园。传感器节点分布在葡萄园的每个角落，每隔一分钟检测一次土壤温度、湿度或该区域有害物的数量，以确保葡萄可以健康生长，如图 1-7 所示。研究人员发现，葡萄园气候的细微变化可极大地影响葡萄酒的质量。通过长年的数据记录以及相关分析，能精确地掌握葡萄酒的质地与葡萄生成过程中的日照、温度、湿度的确切关系。这是一个典型的精准农业、智能耕作的实例。



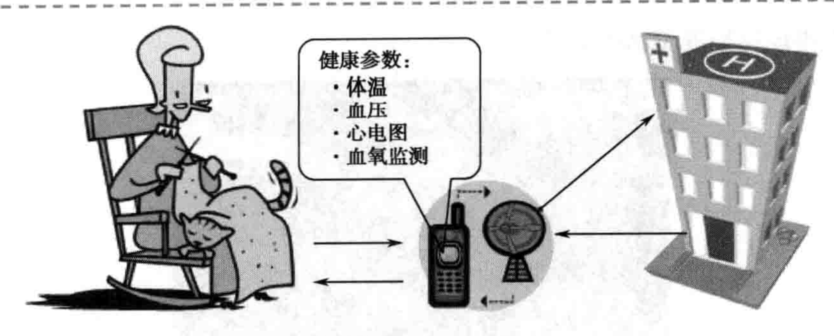


图 1-6 健康智能监控系统

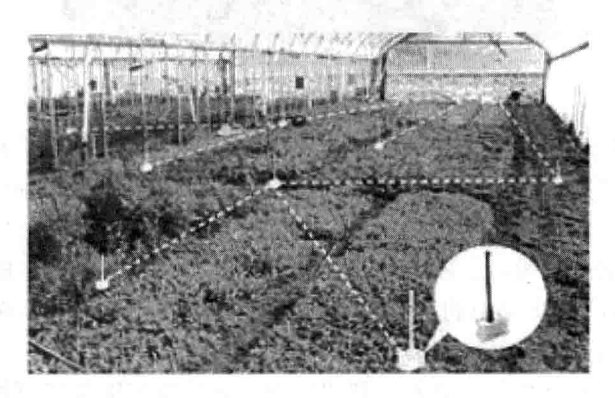


图 1-7 葡萄园环境监测系统

（中国物联网知识普及网：http://www.chinawlw.net.cn）

● 畜牧溯源。给放养牲畜中的每一只羊都贴上一个二维码，这个二维码会一直保持到超市出售的肉品上，消费者可以通过手机阅读二维码，知道牲畜的成长历史，包括羊的种类、产地、出栏时间等，如图 1-8 所示，确保食品安全。我国已有 10 亿存栏动物贴上了这种二维码。

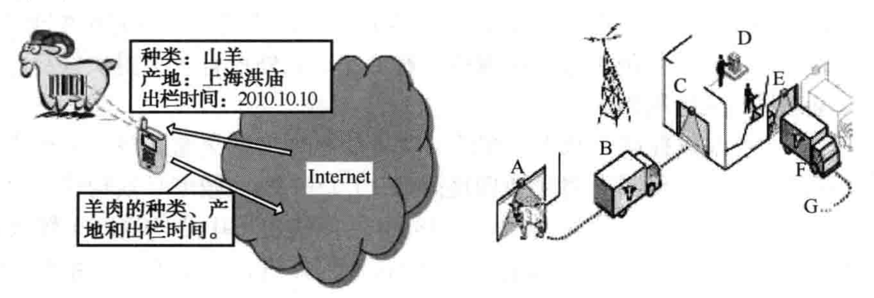


图 1-8 羊肉的跟踪系统

● 文物保护。对珍贵的古老建筑进行保护，是文物保护单位长期以来的一个工作重点。将具有温度、湿度、压力、加速度、光照等传感器的节点布放在重点保护对象当中，无须接线钻孔，便可有效地对建筑物进行长期的监测，如图 1-9 所示，此外，对于珍贵文物而言，在保存地点的墙角、天花板等位置，监测环境的温度、湿度是否超过安全值，可

以更妥善地保护展览品的品质。

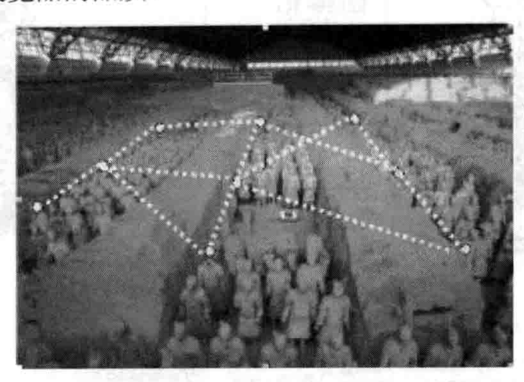


图 1-9　文物环境监控系统

- 智能保姆。当您在办公楼里忙碌时，是否担心在学校上学的孩子的安全？你可以给孩子佩戴一块“智能定位”手表，然后在办公电脑中的电子地图上画一个“电子围栏”，一旦孩子的活动范围超越你设定的区域，你将收到一个报警短信。当辛苦工作了一整天的您准备下班回家的时候，是否想过用手机简单地发出一条指令，提前指挥冬天里停在室外的汽车化雪解冻，让家中的空调启动、电饭煲开始煮饭、解除不在家时的防盗设置呢？这些都是物联网技术已经可以实现的应用。
- 如果在汽车和汽车钥匙上都植入微型感应器，酒后驾车现象就可能被杜绝。当喝了酒的司机掏出汽车钥匙时，钥匙能通过气味感觉器察觉到酒气，并通过无线信号通知汽车“不要发动”，汽车会自动罢工，并能够“命令”司机的手机给其亲友发短信，通知他们司机所在的位置，请亲友来处理。
- Nike 和 Adidas 通过物联网健身产品为跑步者提供帮助：Nike+跑步鞋上有一个传感器，可以跟踪你的跑步，然后把跑步数据发送到 iPod 上。该产品甚至还有自己的社交网络：它可以自动发布状态消息到 Twitter 和 Facebook。Adidas miCoach PACER 是一套售价 $140 的跑步装备，其中包括一个心律检测器和一个跑步传感器（跟鞋配套），该装置可以用语音提示跑步者在跑步过程中保持目标心率。此外还有一个提供健身计划、设定目标、跟踪进度的支持网站。
- 斯德哥尔摩通过收取拥堵费减少了车流。瑞典斯德哥尔摩交通拥挤非常严重，因此道路交通管理部门决定采取措施将交通拥挤降低 10%～15%。城市必须构建一套系统，自动向在周一至周五（节假日除外）6:30 到 18:30 之间进出市中心的注册车辆收税。通过使用 RFID 技术以及利用激光、照相机和系统技术的先进自由车流路边系统，他们设计并实施了一个随机应变的解决方案，可以检测、标识车辆，并收取费用。效果显著：交通拥堵降低了 25%（远远高于预期目标），交通排队所需的时间下降 50%，出租车收入增幅超过了 10%，城市污染级别下降 10%～15%。并且，每天新增四万名公共交通工具乘客。
- 国际快递巨人联邦快递在 2009 年 12 月份为包裹推出了一种新型跟踪装置和网络服务，名字叫做 SenseAware，它可以显示包裹的温度、地点和其他重要信息，比如是否被打开过或被玩耍过。目前联邦快递已经和 50 家保健公司和生命科学公司展开了试点合作，



用于跟踪手术工具包，医疗设备和器官等。

- 惠普实验室打算建立一个“地球中枢神经系统”(CeNSE)。该科研项目的目标是，通过数十亿个“微型、廉价、结实和异常敏感的探测器”建立一个全球感应网络。该计划幕后的技术支持是由惠普实验室的纳米感应研究提供的。这些传感器和 RFID 芯片类似，但是这些微型加速器可以发现移动和振动。惠普实验室称第一个 CeNSE 传感器的敏感度大约为 Wii、iPhone 或汽车气囊系统的敏感度的 1000 倍。以后他们还将推出感应光、温度、气压、气流和湿度的传感器。
- 盖茨之家。比尔•盖茨（Bill Gates）的智能之家（Smart Home）位于美国华盛顿州 Medina 湖畔（见图 1-10），建于 20 世纪 90 年代，耗资 1.13 亿美元，整座建筑物埋设了 52 英里长的电缆和光纤，几乎所有设施都通过网络连接在一起：大门外装有天气感知器，可以根据各项气象指标通知空调系统控制室内温度和通风情况；主人在回家途中只要打个电话发布指令，家里的浴缸便开始放水调温，做好为主人洗去一路风尘的准备。尤其特别的是，每个来这里的客人会领到一个含有电子标签的胸针，其中存有每个人对温度、湿度、灯光等的喜好。当您走进一个房间，电子标签都会通过传感系统与周围设备交流，房间内的温度会调整到您感觉舒适的程度。厨房内，装有一套全自动烹调设备。而厕所里安装了一套检查身体的电脑系统，如发现异常，电脑会立即发出警报。地板能在 6 英寸的范围内跟踪到人的足迹，在有人时自动打开照明，离去的同时自动关闭……

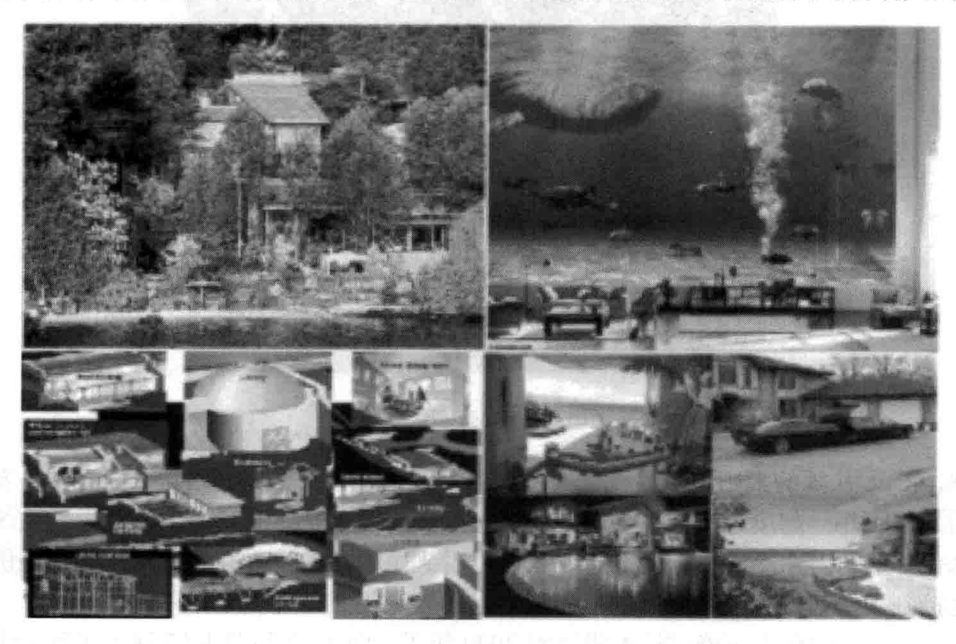


图 1-10　比尔•盖茨之家

国家电信联盟（ITU，International Telecommunication Union）在 2005 年发布的“物联网”报告中，描绘了与前面所述类似的 2020 年日常生活的一天。一个来自西班牙的 23 岁名叫 Rosa 的学生，刚刚同男朋友吵架，想要独处一段时间。她决定私自架驶自己的智能丰田车去法国阿尔卑斯（Alps）山的一个滑雪胜地度周末。但是她必须先去汽车修理厂，因为汽车的 RFID 传

感系统（法定要求安装）提醒她轮胎可能坏了。当她进入修车厂入门通道的时候，基于传感器和无线电技术的诊断工具为她的车进行了全面的检查，并根据检查结果引导她的车开进了一个匹配的配备有自动机器人手的专门修理站点。Rosa 放下车后去喝杯咖啡，饮料自动售卖机知道 Rosa 喜欢冰咖啡，所以在 Rosa 挥舞网络手表付过账之后她得到了一杯她想要的冰咖啡。当 Rosa 回来时，一对新的后备轮胎（装有集成 RFID 标签，可以检测压力、温度和变形情况）已经安装好。机器人然后提示 Rosa 新轮胎上与隐私相关的选项，存储在汽车控制系统中的信息是为维护维修用的，但在汽车行驶中如果周围有 RFID 读卡器，这些信息将被读取到。Rosa 不想任何人知道（特别是她的男友）她要去哪里，所以她选择把这些信息设置为被保护的，防止被无权限的人看到。

终于，Rosa 可以开车去最近的商业街购物了。她想买个有内嵌媒体播放器和温度调节功能的单板滑雪服。由于她要去的滑雪场用无线传感网络监测雪崩的可能性，所以她感到去那里很安全。在通过法国和西班牙边境时，她不需要停留，因为她的车里就存了她的驾驶执照和护照等信息，在超过边境的时候，这些信息被自动传输到简化的边境控制装置中，自动检查放行。这个过程如图 1-11 所示。

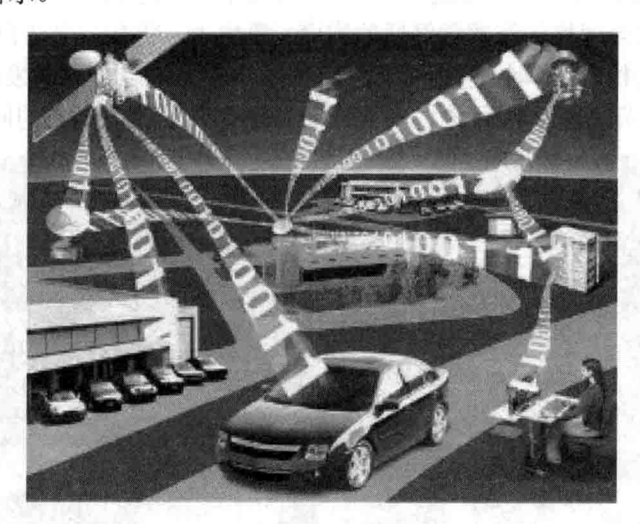
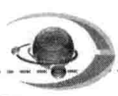


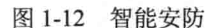
图 1-11　Rosa 智能之旅

突然，Rosa 从她的太阳镜上收到一个视频寻呼，她赶紧把车停到路边，她看到男友正请求原谅并问她是否想一起度过周末。这时她心情正好不错，于是她脱口而出，对导航系统发出了撤掉隐私保护的语音命令，这样她的男友就可以看到她现在的位置并赶过来。即使在所有的事物都被连接到了一起的智能物联网的世界里，人的感觉仍然是起主导作用的。

其实，这一天的到来可能已经不用等到 2020 年了，图 1-12 和图 1-13 展示了我们中国目前已可以做到的物联网生活场景：家中保险柜被保姆不小心碰到，内置设备会“开口说话”，及时向主人手机发出提示信息；机密文件锁在保险柜，若钥匙丢失，管理者用手机发条指令，待命的保险柜便会立即开启；安防部门调用枪支，管理人员并不需枪支编号登记，而只需登录内部网管理模块，便能实现远程开锁授权，实时了解枪柜使用情况……这不是科幻电影中的镜头，而是正在大步向我们走来的保险柜“物联网时代”的美好生活。






图 1-12 智能安防

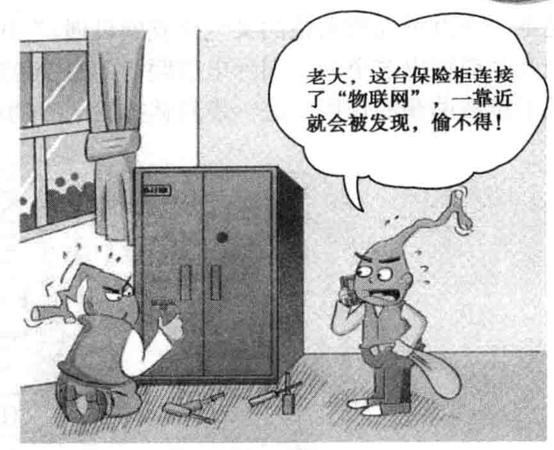


图 1-13 智能枪弹柜

1.2 物联网概述

1.2.1 物联网与相关术语

什么是物联网？顾名思义，本来是一个很简单、易理解的概念。但自从温家宝发表了“感知中国”的讲话后，各行各业的从业人员都争先恐后地站出来发表自己的理解，一时间众说纷纭，莫衷一是，业界和社会上目前对这个概念的理解似乎已形成一种“盲人摸象”的状态。

“The **Internet of things**, also known as the **Internet of objects**, refers to the networked interconnection of everyday objects. It is described as a self-configuring wireless network of sensors whose purpose would be to interconnect all things. The concept is attributed to the former Auto-ID Center, founded in 1999, based at the time at the Massachusetts Institute of Technology (MIT).”

上面是维基百科对物联网的英文定义，从这个简单定义中，“物联网”基本上就是英文“the Internet of Things”的中文直译。在英文中，Internet（互联网）是一个“新词”，由“INTER-NETworking”缩写而得来，不管是英文还是中文，叫起来都很“顺口”且“响亮”。在中文中，虽然“物联网”这个词和“互联网”一样，叫起来很响，但在英文中“物联网”(Internet of Things）不是一个词，叫起来也不“顺口”，所以在英文世界，“物联网”叫得并不响，在不同场合会被其他不同的词所替代，如 M2M（Machine to Machine)、传感网（Senwsor Networks)、智慧地球（Smart Planet 或 Smart Earth)、泛在计算（Pervasive Computing)、普适计算（Ubiquitous Computing）等，还有一些不常用的说法：Sentient Computing（感知计算)，Haptic Computing，Physical Computing，Ambient Intelligence，Utiity Computing，Context-Aware Computing，Things that Think，Machine that Talks，Smart Device 等，如图 1-14 所示。

“Internet of Things”一词最早应该是麻省理工学院（MIT）研究 RFID 的 Auto-ID 中心主任 Ashton 教授 1999 年提出来的。同年，在美国召开的移动计算和网络国际会议也提出：“传感网

是下一个世纪人类面临的又一个发展机遇。”1955 年比尔·盖茨的《未来之路》一书中并未完全表达或提出这个词。国际电信联盟 ITU 2005 年的报告对“Internet of Things”这个词的普及起了推波助澜的作用，进一步具体描绘了“物联网”的时代图景。



图 1-14　物联网相关概念

在美国，专业技术人员更习惯把物联网的事说成 M2M，因为这个词更符合英语习惯，和大家熟悉的 B2B 和 B2C 等词的表达方式类似。从 2004 年开始，美国 M2M 国际组织每年都有一到两次 M2M 国际展会（M2M EXPO）。在当时，提 M2M 或物联网等词在国内都还不被人接受，而提“数字城市”、“两化融合”等词更容易被接受。对于 M2M，有人说，物联网的“Thing”比 M2M 的“Machine”涵盖的范围更广，其实，M2M 中的“Machine”一词也是一个泛指，应该是指任何带有智能芯片的“智能物件”，没有“智能芯片”的“Thing”是“死”的，也不能构成“物联网”。

物联网涉及的范围很广，在美国，除 M2M 外，目前最受关注的物联网领域是 Smart Grid（智能电网）和 Telehealth（远程医疗），这两个领域都能推动奥巴马政府低碳经济和医疗改革。

物联网的一般定义（见图 1-15）是：通过射频识别（RFID）、红外感应器、全球定位系统（GPS）、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。物联网有时被称为传感网，通过装置在各类物体上的电子标签、传感器、二维码等，经过接口与无线网络相连，从而给物体赋予智能，可以实现人与物体的沟通和对话，也可以实现物体之间的沟通和对话。

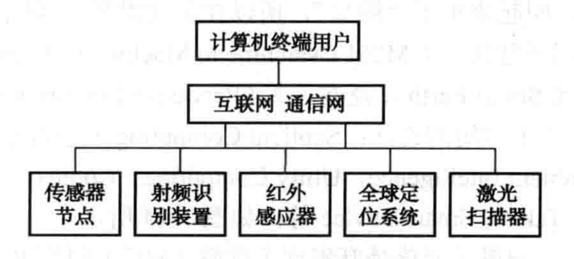


图 1-15　物联网的定义



2010 年温家宝在十一届人大三次会议上所作的政府工作报告中对物联网做了这样的定义：物联网是指通过信息传感设备，按照约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

除了上面的定义之外，还有一些相关组织给物联网做出了如下的定义。

欧盟对物联网的定义：将现有的互联的计算机网络扩展到互联的物品网络。

国际电信联盟（ITU）对物联网的定义：物联网主要解决物到物（Thing to Thing，T2T）、人到物（Human to Thing，H2T）、人到人（Human to Human，H2H）之间的互连。这里与传统互联网不同的是，H2T 是指人利用通用装置与物品之间的连接，H2H 是指人与人之间不依赖于个人计算机而进行的互连。需要利用物联网才能解决的是传统意义上的互联网没有考虑的、对于任何物品连接的问题。

ITU 物联网研究组对物联网的定义：物联网的核心技术主要是普适网络、下一代网络和普适计算。这 3 项核心技术的简单定义如下：普适网络，无处不在的、普遍存在的网络；下一代网络，可以在任何时间、任何地点、互连任何物品，提供多种形式信息访问和信息管理的网络；普适计算，无处不在的、普通存在的计算。其中下一代网络中“互连任何物品”的定义是 ITU 物联网研究组对下一代网络定义的扩展，是对下一代网络发展趋势的高度概括。从现在已经成为现实多种装置的互连网络，如手机互连、移动装置互连、汽车互连、传感器互连等，都揭示了下一代网络在“互连任何物品”方面的发展趋势。

1.2.2 互联网、物联网与物连网

如果我们仔细研究“互联网”这个中文名词，不难发现，在翻译“Internet”这个词的时候，我们并没有“忠实”于英文原意。Internet 在英文中的原意指的是“Network of Networks”，中文直译应该是“互连网”，强调“连接”的本意。当时翻译成“互联网”，强调“联合”，所以中文的意思就比英文原词意义更丰富，也更接近 Internet 发展的趋势和目前的现状。

同样，在“物联网”这个词的翻译上，人们又“超前”了，就目前的现状来说，用“物连网”这个词（或 M2M）更确切。目前国内外做的许多工作，也只能算是“物连网”（Network of Things），由于网络安全和应用本身的特点等原因，大多数应用都运行在内网（Intranet）和专网（Extranet）中。如果是“物联网”，顾名思义就是要上公网 Internet，许多应用是不可能做成“物联网”供大众去浏览和查询的。但有些东西的确是可以做成“物联网”的，如 Google 的 PowerMeter，所以国外有些人提出了 X-Internet 的概念，也就是 eXcutable and eXtendable Internet（可执行和可扩展的互联网）。

人们一般把互联网称为“外网”，此外还有上面提到的内网和专网。互联网是一个“平台”，着重于“互联互通”和信息共享，而物联网则不同，既然有“物”，就一定有产权和归属权，共享也一定是有条件的。所以，在相当长时间内，“物联网”主要将以“物连网”的形式存在于内网和专网中。

物联网和互联网还有一个显著的区别，就是目前在互联网上的“内容”，绝大部分都是“人工输入”的，而物联网上的内容将主要是“工业化”和“自动化”两化融合的机器“自动生成”的。同时，我们也应该看到，互联网目前是以有线 TCP/IP 协议为主要载体的，而物联网的很

多应用更依赖于“无线网络”技术，各种短距离无线通信技术（包括 RFID 和 Mesh 等）和长距离的无线通信技术（GSM 和各种 CDMA 等）是目前物联网产业发展的主要基础设施。

1.2.3 物联网发展史

- 物联网（The Internet of things）的概念是在 1999 年提出：Foundation of Auto-ID center of MIT（RFID technology）（见图 1-16）。
- 2003 SUN article：Toward a Global “Internet of Things”。
- 2005 年 11 月 17 日：在突尼斯举行的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布《ITU 互联网报告 2005：物联网》。
- 2009 年 1 月 23 日：IBM Smart Planet，奥巴马针对 IBM 首席执行官彭明盛首次提出“智慧地球”这一概念做出回应：物联网技术是美国在 21 世纪保持和夺回竞争优势的方式。
- 2009 年 8 月 7 日：温家宝考察中科院无锡高新微纳传感网工程技术研发中心，强调“在传感网发展中，要早一点谋划未来，早一点攻破核心技术，把传感系统和 3G 中的 TD 技术结合起来”。
- 2009 年 9 月 21 日：工信部在相关会议上，首次明确提出要进一步研究建设物联网、传感网，加快传感中心建设，推进信息技术在工业领域的广泛应用，提高资源利用率、经济运行效益和投入产出效率等。
- 2009 年 9 月：Internet of Things – An action plan for Europe，欧盟行动计划。

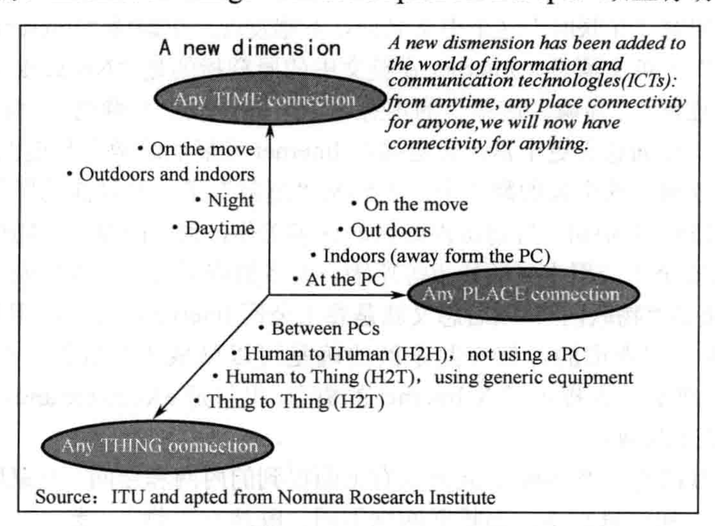


图 1-16 物联网新维度

1.3 物联网的关键技术

国际电信联盟（ITU）将射频识别技术（RFID）、传感器技术、纳米技术、智能嵌入技术列



为物联网关键技术。其中，RFID 也被公认为是物联网的构建基础和核心。中科院软件研究所专家认为，物联网的关键技术包括物体标识、体系架构、通信和网络、安全和隐私、服务发现和搜索、软硬件、能量获取和存储、设备微型小型化、标准。

物联网是在计算机互联网的基础上，利用 RFID、无线数据通信等技术，构造一个覆盖世界上万事万物的网络。在这个网络中，物品能够彼此进行“交流”，而无须人的干预。其实质是利用 RFID 技术，通过计算机互联网实现物品自动识别和信息的互联与共享。而 RFID，正是能够让物品相互沟通的一种技术。在物联世界中，RFID 标签中存储着规范而具有互用性的信息，通过无线数据通信网络把它们自动采集到中央信息系统，实现物品的识别，进而通过开放性的计算机网络实现信息交换和共享，实现对物品的“透明”管理。

物联网概念的问世，打破了之前的传统思维。过去的思路一直是将物理基础设施和 IT 基础设施分开：一方面是机场、公路、建筑物，而另一方面是数据中心、个人电脑、宽带等。而在物联网时代，钢筋混凝土、电缆将与芯片、宽带整合为统一的基础设施，在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。

1.4　物联网工程的基本架构

物联网技术是一项综合性的技术，它的开展具有规模性、广泛性、管理性、技术性、物的属性等特征，其实现步骤可分为感知层、传输层、应用层三个层次（见图 1-17）。

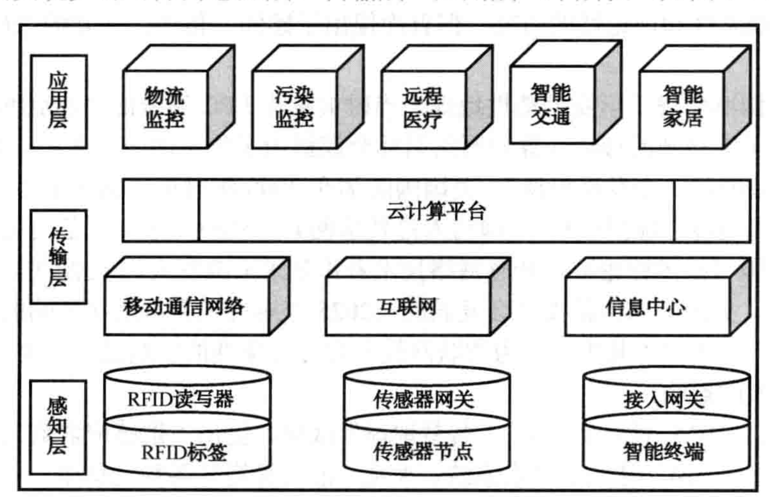


图 1-17　物联网结构

感知层主要包括二维码、标签和识读器、RFID 标签和读写器、摄像头、GPS、传感器以及 M2M 终端、传感器网络和传感器网关等，实现物体的感知、识别，采集、捕获信息。感知层要突破的方向是具备更敏感、更全面的感知能力，解决低功耗、小型化和低成本的问题。

网络层包括各种通信网络与互联网形成的融合网络，是相对成熟的部分，现有可用的网络包括互联网、广电网络、通信网络等。但在 M2M 应用大规模普及后，仍然需要解决新的业务

模型对系统容量、QoS（Quality of Service，服务质量）的特别要求。另外，物联网管理中心、信息中心、云计算平台、专家系统等对海量信息进行智能处理亟待突破。网络层是物联网成为普遍服务的基础设施，有待突破的方向是向下与感知层的结合，向上与应用层的结合。

应用层是将物联网技术与行业专业领域技术相结合，实现广泛智能化应用的解决方案，利用现有的手机、PC、PDA、iPad 等终端实现应用。物联网通过应用层最终实现信息技术与行业专业技术的深度融合，对国民经济和社会发展具有广泛影响。应用层的关键问题在于信息的社会共享，以及信息安全的保障。

公共技术不属于物联网技术的某个特定层面，而是与物联网技术架构的三层都有关系，它包括标识与解析、安全技术、网络管理和服务质量管理。

1.5 物联网发展现状

1.5.1 国外发展情况

1. 美国

作为物联网发展排头兵的 RFID 技术，早在第二次世界大战时期就出现了，后来在美国对伊拉克战争中得到大量使用，用于管理军需后勤物资。1991 年由美国提出普适计算的概念，尽管总体来说它是概念性和理论性的研究，但首次提出了感知、传送、交互的三层结构，是物联网的雏形。

1998 年，美国麻省理工学院创造性地提出当时被称作 EPC 系统的“物联网”概念。

1999 年，在美国召开的移动计算和网络国际会议提出了传感网的概念，认为“传感网是下一个世纪人类面临的又一个发展机遇”。美国国防部在 2000 年时把传感网定为 5 大国防建设领域之一，仅在美墨边境“虚拟栅栏”（即防入侵传感网）上就投入了 470 亿美元。

2003 年，美国《技术评论》将传感网络技术看作是未来改变人们生活的十大技术之首。

2008 年 7 月，美国国家情报委员会发表的《2025 年对美国利益潜在影响的 6 种关键技术》报告将“物联网”技术列入其中，认为物联网技术存在裂变性的影响能力，将对人类社会的生产和生活带来巨大的影响。

2008 年 11 月，IBM 对外公布了 “智慧地球”战略，提出“把感应器嵌入和装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道等各种物体中，并且被普遍连接，形成所谓‘物联网’，并通过超级计算机和云计算将‘物联网’整合起来，实现人类社会与物理系统的整合。”

2008 年 12 月，奥巴马向 IBM 咨询了“智慧地球”的有关细节，并共同就投资智能基础设施对于经济的促进效果进行了研究。

2009 年 1 月 7 日，IBM 与美国智库机构信息技术与创新基金会（ITIF）共同向奥巴马政府提交了“The Digital Road to Recover: A Stimulus Plan to Create Jobs，Boost Productivity and Revitalize America”，提出通过信息通信技术（Information and Communication Technology，ICT）



投资可在短期内创造就业机会，美国政府只要新增300亿美元的ICT投资（包括智能电网、智能医疗、宽带网络三个领域），便可以为民众创造出94.9万个就业机会。

2009年1月28日奥巴马与美国工商业领袖举行了一次“圆桌会议”。奥巴马发表讲话，肯定了这一思路：“经济刺激资金将会投入到宽带网络等新兴技术中去，毫无疑问，这就是美国在21世纪保持和夺回竞争优势的方式。”并进一步将问题上升到美国国家政策层面。

2009年2月17日奥巴马签署生效的《恢复和再投资法案》(Recovery and Reinvestment Act，美国的经济刺激计划)，批准推进“智慧地球”中两个领域的发展——智慧的电网和智慧的医疗，分别批准投资为110亿和190亿美元；同时批准宽带网络投资72亿美元。

2010年至2011年间，美国先后颁布了关于政府机构采用云计算的政府文件以及《联邦云计算策略》白皮书，积极推广云计算在政府各部门的应用。

2. 欧盟

2000年3月在葡萄牙的里斯本举行的欧洲首脑特别会议上，欧洲理事会提出了一个未来十年的战略目标——使欧盟成为世界上最有竞争力、经济最活跃的知识经济体。为此，欧盟具体实施了一个行动计划——“e- Europe”，建设“为所有人的信息社会”(Information Society for all)。

2005年6月1日，欧盟委员会在比利时的布鲁塞尔公布了一个新的战略计划——Initiative “i2010: European Information Society 2010”，其目的在于促进欧盟经济增长和创造就业。

2006年3月，欧盟召开会议“From RFID to the Internet of Things”，对物联网做了进一步的描述。

2008年在法国召开的欧洲物联网大会的重要议题包括未来互联网和物联网的挑战、物联网中的隐私权、物联网在主要工业部门中的影响等内容。

2009年，欧盟发布了下一代全欧移动宽带长期演进与超越以及ICT（information and communications technology）研发与创新战略，欧盟计划在未来10年将欧洲ICT研究与创新投资加倍。

2009年6月18日，欧盟委员会发布了世界第一个物联网发展战略——《欧盟物联网行动计划》(Internet of Things An action plan for Europe)，描绘了物联网技术应用的前景，并提出要加强欧盟政府对物联网的管理，消除物联网发展的障碍。

2009年11月，欧洲联盟发布了《未来物联网战略》。除了通过信息与通信技术研发计划投资4亿欧元、90多个研发项目提高网络智能化水平，欧盟委员会还将于2011—2013年间每年新增2亿欧元进一步加强研发力度，同时拿出3亿欧元专款，支持物联网相关公私合作短期项目建设。

2009年12月15日，欧洲物联网项目总体协调组发布了《物联网战略研究路线图》，将物联网研究分为感知、宏观架构、通信、组网、软件平台及中间件、硬件、情报提炼、搜索引擎、能源管理、安全10个层面，系统地提出了物联网战略研究的关键技术和路径。

2010年6月，欧盟委员会推出了《数字议程》(Digital Agenda) 5年行动计划，该议程是《欧盟2020战略》7项旗舰举措中的一项。

2012年7月10日，欧盟委员会启动了“智能城市和社区欧洲创新伙伴行动”(Smart Cities and Communities European Innovation Partnership，简称SCC-EIP)。

3. 日本

2000 年 7 月，日本政府召开了 IT 战略会议，创立了 IT 战略总部，将其作为国家信息化的集中研究组织。

2001 年 1 月，推行“e-Japan”战略。

2004 年 5 月，提出了“u-Japan”战略计划（ubiquitous，意指“无所不在的”）。“u-Japan”战略的理念是以人为本，实现所有人与人、物与物、人与物之间的连接（即 4U，Ubiquitous、Universal、User-oriented、Unique），希望在 2010 年将日本建设成一个“实现随时、随地、任何物体、任何人均可连接的泛在网络社会”。

2009 年 2 月，日本为应对日渐疲软的经济环境，紧急出台了宏观性的指导政策“ICT 新政”。2009 年 4 月，日本总务省公布了“新政”的实施性文件——“数字日本创新计划”（ICT Hatoyama Plan，亦称 ICT 鸠山计划）纲要，将其作为未来 3 年中优先实施的政策。

2009 年 7 月 6 日，日本 IT 战略本部发表了“I-Japan 战略 2015”，目标是“实现以国民为主角的数字安心、活力社会”。I-Japan 战略中提出重点发展的物联网业务包括：通过对汽车远程控制、车与车之间的通信、车与路边的通信，增强交通安全性的下一代 ITS 应用；老年与儿童监视、环境监测传感器组网、远程医疗、远程教学、远程办公等智能城镇项目；环境的监测和管理，控制碳排放量。

2010 年 5 月 17 日，日本总务省发布了“智能云研究会报告书”，制定了“智能云战略”，目的在于借助云服务，推动整体社会系统实现海量信息和知识的集成与共享。

4. 韩国

自 1997 年起，韩国政府出台了一系列推动国家信息化建设的产业政策，包括 RFID 先导计划、RFID 前面推动计划、USN（传感器网）领域测试计划等。

1999 年，韩国信息通信部出台了《2000 年国家社会信息化推进计划》，围绕“十大知识信息强国”的目标。

2003 年，韩国政府启动了旨在使韩国科技产业保持竞争力的“IT839”计划。韩国于 2002 年 4 月提出了 e-Korea（电子韩国）战略，其关注的重点是加紧建设 IT 基础设施，使得韩国社会的各方面在尖端科技的带动下跨上一个新的发展台阶。

2004 年，韩国信息通信产业部（MIC）主导成立了 u-Korea（ubiquitous society，无所不在的社会）策略规划小组，并于 2006 年确立了 u-Korea 的政策方针。u-Korea 主要分为发展期与成熟期两个执行阶段。发展期（2006—2010 年）的重点任务是基础环境的建设、技术的应用以及 u 社会制度的建立；成熟期（2011—2015 年）的重点任务为推广 u 化服务。

2005 年韩国信通部推出《数字时代的人本主义：IT839 战略》（Humanism in the Digital World: IT839 Strategy）U-IT839 战略以具体呼应 u-Korea。

2008 年 12 月，韩国新政府《国家信息化基本计划》出炉，韩国将在 2012 年年底前，把上网速度提高到目前的 10 倍，并建立 10 处产学研汇集的信息科学技术中心区。

2009 年 6 月，韩国通信委员会（KCC）决定促进未来物体通信网络建设，实现用户随时随地安全方便地进行人与物、物与物之间的智能通信。



2009 年 10 月 13 日，韩国出台了《物联网基础设施构建基本规划》，将物联网市场确定为新增长动力，提出到 2012 年实现“通过构建世界最先进的物联网基础实施，打造未来广播通信融合领域超一流信息通信技术强国”目标。

2010 年，韩国政府陆续出台了推动 RFID 发展的相关政策，为使其成为 RFID 和传感网行业世界前三强进行努力。

2010 年 9 月，韩国通信委员会（KCC）确立了到 2012 年“通过构建世界最先进的传感器网基础实施，打造未来广播通信融合领域超一流 ICT 强国”的目标。

1.5.2 国内发展情况

在中国，“物联网”最早被称为“传感网”，中国的传感网发展起步较早，中科院早在 1999 年就启动了传感网研究，先后投入数亿元，在无线传感网络、智能微型传感器、现代通信技术等方面取得了重要进展。

2004 年，国家金卡工程办公室把 RFID 产业发展与行业应用列入国家金卡工程的重点工作。

2005 年 4 月 27 日，中国 RFID 产业联盟正式宣布成立。

2005 年 10 月原信息产业部批准成立了“电子标签标准工作组”，开展电子标签标准的研究。

2005 年发布的《国家中长期科学和技术发展规划纲要（2006—2020 年）（国发[2005]第 044 号）》就早已明确将传感网作为重点领域和优先主题。2006 年 23 个部门（行业）共同成立了国家金卡办 RFID 应用工作组，启动了相关 RFID 应用试点工作。

在 2006 年底，中国移动物联网运营中心即在重庆成立。

2008 年上半年无锡市与中科院上海微系统研究所合作成立中科院无锡微纳传感网工程技术研发中心，大力推进传感网、物联网产业化进程。

2009 年 6 月 10 日，中国科学院发布的“创新 2050：科学技术与中国的未来，中国至 2050 年信息科技发展路线图”描述了物联网的发展路线图。

2009 年 8 月 7 日，国务院总理温家宝到无锡微纳传感网工程技术研发中心视察。

2009 年 11 月 3 日，温家宝在人民大会堂向首都科技界发表了题为《让科技引领中国可持续发展》的讲话。他提出：“要着力突破传感网、物联网关键技术，及早部署后 IP 时代相关技术研发，使信息网络产业成为推动产业升级、迈向信息社会的‘发动机’”。

2009 年 9 月 11 日，经国家标准化管理委员会批准，全国信息技术标准化技术委员会组建了“物联网”标准工作组。

2009 年 9 月国家发展和改革委员会、工业和信息化部发布《关于进一步做好电子信息产业振兴和技术改造项目组织工作的通知》，RFID、物联网等作为计算机产业及下一代互联网关键技术，被列为重点支持领域。

2009 年 9 月 10 日，全国高校首家物联网研究院在南京邮电大学正式成立。

2009 年 11 月 3 日，无锡建设国家传感网创新示范区（国家传感信息中心）获国务院批准。

在工信部 2010 年 2 月 2 日公告的 62 个国家新型工业化产业示范基地中，江苏无锡高新技术产业开发区已经正式获批为物联网示范基地。

2010 年 3 月 2 日，上海物联网中心在上海市嘉定区揭牌，中心将依托中国科学院上海微系

统与信息技术研究所，实施物联网中心研发基地建设。

2010年6月8日，中国物联网标准联合工作组在北京成立，以推进物联网技术的研究和标准的制定。

2010年6月22日，在上海开幕的2010中国国际物联网大会上，工业和信息化部称，物联网已正式列入国家重点发展的5大战略性新兴产业之一。

2011年5月20日，工信部电信研究院科研团队在北京举办了《中国物联网白皮书（2011）》发布会，向全社会公开研究成果。

2012年3月30日，中国提交的“物联网概述”标准草案，经国际电信联盟审议通过，成为了全球第一个物联网总体性标准。这次中国标准的“被采纳”不仅标志着在国际物联网领域中国的话语权大大增强，也预示着中国物联网产业将进入发展新阶段。

1.6 物联网工程面临的问题

1.6.1 技术问题

纵观全球物联网中枢之一的RFID技术与产业，我国已经在高频应用领域占据了世界第一的位置，形成了从芯片设计、制造、封装和读写器设计、制造到应用的成熟的产业链。而在国际上重点发展的超高频领域，我国与国际先进水平相比，还存在着5大瓶颈。

1. 企业技术研发水平薄弱

目前，我国进入RFID领域的企业基本都是中小型的企业，企业资金实力相对薄弱，用于技术研发的资金很受限制，大大影响到企业的技术创新。

2. RFID标签成本过高，限制了其应用范围的扩大

目前，制作一个标签的成本大约在1.5元左右，高额成本决定了这项技术目前只能应用在附加值相对较高的商品上，比如汽车、高档酒、门票等方面，而在低价值商品上则无法推广，这大大限制了RFID应用范围的推广。

3. 缺乏国家标准

目前在高频领域我国主要沿用国标标准，但在关键的超高频领域，标准仍由国外组织控制着，我国如果照搬这个标准，未来将要支付大量的专利费用，这将增加中国企业的成本。因此，尽快制定出自己的超高频RFID标准迫在眉睫。

4. 个人隐私问题

在物联网中，射频识别技术是一个很重要的技术。在射频识别系统中，标签有可能预先被嵌入任何物品中，比如人们的日常生活物品中，但由于该物品（比如衣物）的拥有者，不一定能够觉察该物品预先已嵌入有电子标签以及自身可能不受控制地被扫描、定位和追踪，这势必



会使个人的隐私受到侵犯。因此，如何确保标签物的拥有者个人隐私不受侵犯便成为射频识别技术以至物联网推广的关键问题。而且，这不仅仅是一个技术问题，还涉及政治和法律问题。这个问题必须引起高度重视并从技术上和法律上予以解决。

造成侵犯个人隐私问题的关键在于射频标签的基本功能：任意一个标签的标识（ID）或识别码都能在远程被任意扫描，且标签自动地、不加区别地回应读写器的指令并将其所存储的信息传输给读写器。这一特性可用来追踪和定位某个特定用户或物品，从而获得相关的隐私信息。这就带来了如何确保嵌入有标签的物品的持有者个人隐私不受侵犯的问题。

5. 国家安全

物联网产业将是万亿元级规模的产业，是把“双刃剑“。物联网推动经济和社会发展的同时，将对国家安全问题提出挑战。因为物联网将涵盖的领域包括电网、油气管道、供水等民生和国家战略，甚至包括军事领域的信息与控制。物联网让世界上的万事万物都能参与“互联互通”，不能再采取物理隔离等强制手段来人为地干预信息的交换，对于一个国家或单位而言，也就意味着没有任何家底可以隐藏。如果IBM“智慧地球”实施，如何保证涉及国家安全的信息不被泄露，如何保证企业商业机密、地方政府甚至国家机密不被泄露，都是摆在面前的首要问题。

1.6.2 标准问题

物联网是一个多设备、多网络、多应用、互联互通、互相融合的一个大网，这里面既有传感器、计算机，又有通信网络，需要把所有这些系统都联在一起，因而，所有的接口、通信协议都需要有国家标准来指引。如果没有这个统一的标准，就会使整个产业混乱。从互联网的发展历程来看，统一的技术标准和一体化的协调机制是导致现在互联网能遍布全球的重要原因。标准化体系的建立将成为发展物联网产业的首要先决条件。

谁掌握物联网标准谁就主动。目前已经积极开展与传感网相关的标准化工作的主要标准组织包括ISO/IEC JTC1 WG7、ITU-T、IETF、IEEE 802.15、IEEE 1451、ZigBee等。

2008年6月，首届ISO/IEC传感网国际标准化大会在中国召开，中国代表提出的传感网体系架构、标准体系、演进路线、协同架构等代表传感网发展方向的顶层设计被ISO/IEC国际标准认可，已纳入ISO/IEC SGSN总体技术文档中。

2009年10月，由中国、美国、韩国、德国、法国、英国等国家联合成立了ISO/IEC JTC1传感网标准工作组WG7。

目前，我国物联网技术的研发水平已位于世界前列，在一些关键技术上处于国际领先，与德国、美国、日本等国一起，成为国际标准制定的主要国家，逐步成为全球物联网产业链中重要的一环。在物联网的基础标准领域，中国要积极参与制定国际标准，并按照国际标准建设国内的物联网；同时，尽快着手制定物联网相关标准体系，坚持国际标准和国内标准同步推进的原则，着手研究和制定我国物联网标准，统一技术和接口标准，进一步确立并扩大我国在物联网领域国际标准制定上的发言权。



1.6.3 商业模式完善问题

物联网召唤着新的商业模式。物联网作为一个新生事物，虽然前景广阔、相关产业参与意愿强烈、发展很快，但其技术研发和应用都尚处于初级阶段，且成本还较高。虽然已出现了一些小范围的应用实践，如国内在上海建设的浦东机场防入侵系统、停车收费系统以及服务于世博会的"车务通"、"e 物流"等项目，但是物联网本身还没有形成成熟的商业模式和推广应用体系，商业模式不清晰，未形成共赢的、规模化的产业链。物联网分为感知、网络、应用三个层次，在每一个层面上，都将有多种选择去开拓市场。这样，在未来物联网建设过程中，商业模式变得异常关键。虽然物联网市场前景广阔，但是整个行业目前尚未出现稳定和有利可图的商业模式，也没有任何产业可以在这一点上统一引领物联网的发展浪潮。

物联网涉及终端制造商、应用开发商、网络运营商、系统集成商、最终用户等多个环节。例如在应用环节，物联网耦合度低、附加值低、同质化竞争严重。应用开发商未降低开发成本，往往绑定上游供货商，缺乏竞争机制。其他三个环节也存在一些问题。原有的商业模式需要更新升级来适应规模化、快速化、跨领域化的应用，而更关键的是要真正建立一个多方共赢的商业模式，这才是推动物联网能够长远有效发展的核心动力。

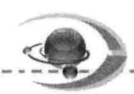
物联网产业链涉及范围广，运营商要通过平台、标准等发挥在产业链中的核心及主导作用，充分调动各方积极性，才能争取更多的主动权。要实现多方共赢，就必须让物联网真正成为一种商业的驱动力，而不是一种行政的强制力，让产业链内所有参与物联网建设的各个环节都能从中获益，获取相应的商业回报，才能够使物联网得以持续快速地发展。

在商业模式上，根据运营主体来分，分成电信自营业务、虚拟运营商业务和合作运营业务。运营商可以采用开放的物联网商业运作模式。对于标准化数据传输业务，应采用电信自营方式，利用运营商自有管道、自有应用系统与管理平台直接面向客户进行销售、安装、维护。对于有较强行业壁垒的客户群，当虚拟运营商具备较大行业资源优势时，可以充分发挥虚拟运营商的能力，合力推广，实现共赢。对于专业特性强，而 SP 具有丰富经验的行业，运营商应采用合作运营的方式。

物联网在中国的发展是一项任重而道远的过程，有着行政与商业双重使命，它的实现将是一个涉及信息技术、社会观念、管理体系、应用模式等多方协调、合作及观念转变的过程，将是一个由点突破，逐步推进的过程。在这一过程中，在政府的引导下，在运营商的主导下，建立多方共赢的商业模式。激发参与者各方的参与热情，使参与各方均有收益，物联网才能够真正拥有长效、可持续发展的动力。

1.7 练习题

1. 请完善如图 1-18 所示的物联网发展历程。并阅读《未来之路》，选取其中感兴趣的内容与大家分享。



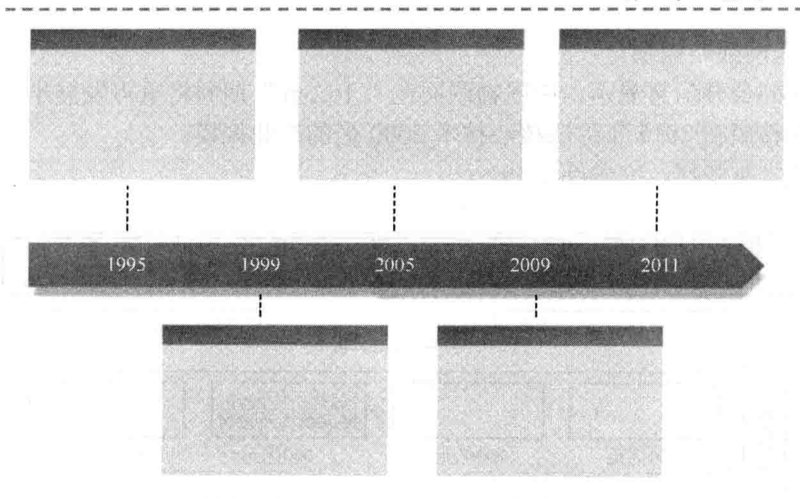


图 1-18　物联网发展历程

2．请给出以下机构对物联网的定义。

● Auto-ID

● 国际电信联盟（ITU）

● 欧洲智能系统集成技术平台（EPoSS）

● 中国政府工作报告

根据以上定义，对于物联网你是怎么理解的呢？请写在以下空白处。

3．中国物联网战略规划。

工信部披露的公开信息显示，中国物联网在“十二五”期间将重点发展十大应用领域、四大核心技术，并希望在 2015 年形成核心技术 2000 亿的产业规模。

请查阅相关文献资料，完善图 1-19。

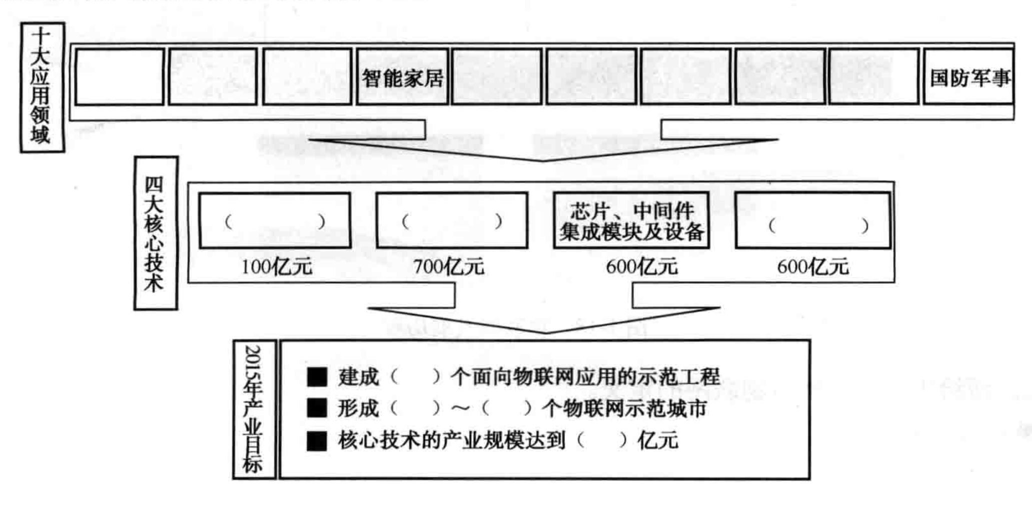


图 1-19　中国物联网战略规划

4．根据物联网三个层次及各层次具体含义填写图 1-20。

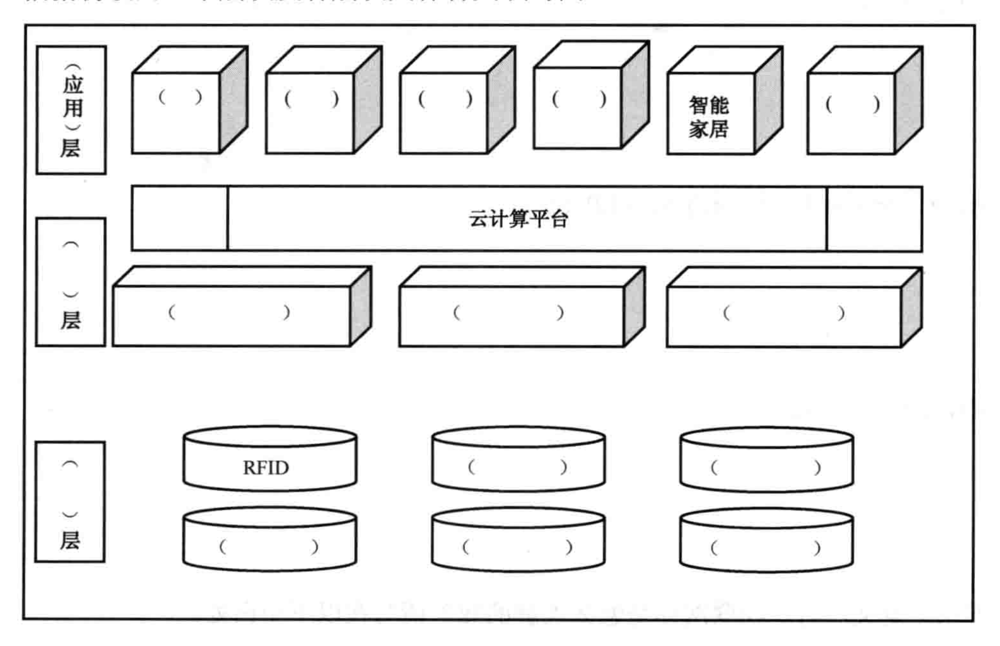


图 1-20　物联网工程的基本架构

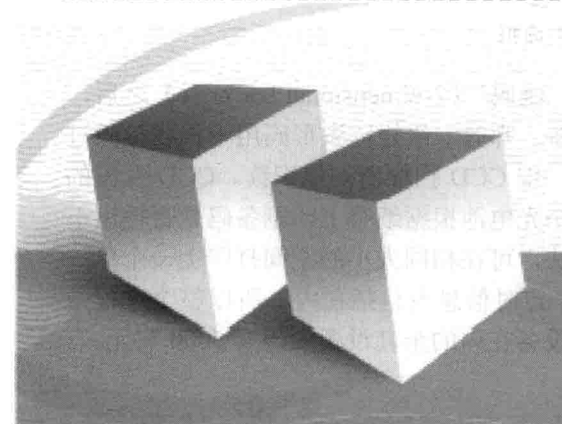
第2章

物联网 RFID 技术

在 20 世纪 20 年代的威斯汀豪斯（Westinghouse）实验室，一位性格古怪的发明家约翰·科芒德（John Kermode）正在思考如何根据邮政编码自动分拣邮件。他的想法是在信封上做条形标记，设计方案非常的简单，即一个“条”表示数字“1”，两个“条”表示“2”……以此类推。然后，他发明了由基本元件组成的条形识别设备：一个能够发射光并接受反射光的仪器（即扫描器），一个测定发射信号的方法（即边缘定位线圈），以及测定结果的方法（即译码器）。科芒德的扫描器利用当时新发明的光电池来收集反射光。“空”反射回来的是强信号，“条”反射回来的是弱信号。与当今高速度的电子元器件应用不同的是，科芒德利用磁性线圈来测定“条”和“空”。就像一个小孩将电线与电池连接再绕在一颗钉子上来夹纸。科芒德用一个带铁芯的线圈在接收到“空”的信号的时候吸引一个开关，在接收到“条”的信号的时候，释放开关并接通电路。因此，最早的条码阅读器噪声很大。开关由一系列的继电器控制，“开”和“关”由打印在信封上“条”的数量决定。通过这种方法，条码符号直接对信件进行分拣。条形码条码分布区域所代表的特定含义如图 2-1 所示。



图 2-1　条形码条码分布区域与含义



科芒德条形码所包含的信息量相当的低，并且很难编出十个以上的不同代码。而其合作者道格拉斯·杨（Douglas Young）使用更少的条，但是利用条之间空的尺寸变化，就像今天的UPC条码（Universal Product Code，统一商品代码）符号使用四个不同的条空尺寸。新的条码符号可在同样大小的空间对一百个不同的地区进行编码，而科芒德码只能对十个不同的地区进行编码。

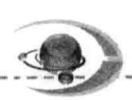
直到1949年的专利文献中才第一次有了诺姆·伍德兰（Norm Woodland）和伯纳德·西尔沃（Bernard Silver）发明的全方位条形码符号的记载，在这之前的专利文献中始终没有关于条形码技术的记录，也没有投入实际应用的先例。诺姆·伍德兰和伯纳德·西尔沃的想法是利用科芒德和杨的垂直的"条"和"空"，并使之弯曲成环状，非常像射箭的靶子。这样扫描器通过扫描图形的中心，能够对条形码符号解码，不管条形码符号方向的朝向。

在对这项专利技术不断改进的过程中，一位科幻小说作家艾萨克·阿西莫夫(Isaac Azimov）在他的《赤裸的太阳》（The Naked Sun）一书中讲述了使用信息编码的新方法实现自动识别的事例。那时人们觉得此书中的条形码符号看上去像是一个方格子的棋盘，但是今天的条形码专业人士马上会意识到这是一个二维矩阵条形码符号。虽然此条形码符号没有方向、定位和定时，但很显然它表示的是高信息密度的数字编码（见图2-2)。



图2-2 《赤裸的太阳》海报

直到1970年Interface Mechanisms公司开发出"二维码"（2-dimensional bar code）之后，才有了价格适于销售的二维矩阵条码的打印和识读设备。那时二维矩阵条形码用于报社排版过程的自动化。二维矩阵条形码印在纸带上，由今天的一维CCD扫描器扫描识读。CCD发出的光照在纸带上，每个光电池对准纸带的不同区域。每个光电池根据纸带上印刷条码是否输出不同的图案，组合产生一个高密度信息图案。用这种方法，可在相同大小的空间打印上一个单一的字符，作为早期科芒德码之中的一个单一的"条"。定时信息也包括在内，所以整个过程是合理的。当第一个系统进入市场后，包括打印和识读设备在内的全套设备大约要5000美元。



此后不久，随着 LED（发光二极管）、微处理器和激光二极管的不断发展，迎来了新的标识符号和其应用的大爆炸（被称为“条码工业”）。今天很少能找到没有直接接触过条形码技术的公司或个人。条形码使我们每一个人的生活都变得更加轻松和方便。

进入 21 世纪，条形码在越来越多的情况下已经不能满足人们的需求。虽然价格低廉，但它有过多的缺点，如读取速度慢、存储能力小、穿透能力弱、适应性不强以及不能进行读写操作等。与此同时，另外一项逐步成熟的识别技术以近乎疯狂的速度一夜之间席卷全球，彻底改变了条形码一统天下的现状，这就是非接触射频识别（RFID）技术。作为条形码的完美替代品，RFID 技术有许多独特优势：防火、穿透性强、读取速度快、识别距离远、存储数据能力大、数据可进行加密、可进行读写等。RFID 技术最大的特点是能够提供更细致、更精确的产品供货信息，并能实现货物供给过程的自动化。

当 RFID 与互联网相结合时，一场影响深远的革命就来临了。特别是，当赋予地球上所有物品以唯一 IP 地址的 IPv6 技术与承载着物品大量相关信息并有无线通信能力的 RFID 相结合时，双方的巨大潜能进一步释放出来，一个人与人、人与物、物与物相互联系的“物联网”诞生了，带来了令人惊叹的能量。

2.1 自动识别技术

2.1.1 光符号识别技术

早在 20 世纪 60 年代，人类就已经开始研究光学符号识别（Optical Character Recognition，OCR），这种让机器按照人类方式来阅读和识别的方法可以算是自动识别技术的先驱。光学符号识别系统最主要的优点是信息密度高，在机器无法识别的情况下人类也可以用眼睛阅读数据。然而，想让机器做对人类来说轻而易举的事情却不那么容易，光学符号识别系统因其价格贵、系统复杂而受到很大的限制。近年来，光符号识别虽然没有在自动识别领域获得成功，却在人工智能机和图像处理等其他领域得到了长足的发展和进步。

OCR 可用于文本资料扫描输入、图像识别、手写汉字识别等。

2.1.2 语音识别技术

语音识别技术，也被称为自动语音识别（Automatic Speech Recognition，ASR），其目标是将人类语音中的词汇内容转换为计算机可读的输入，例如按键、二进制编码或者字符序列。与说话人识别及说话人确认不同，后者尝试识别或确认发出语音的说话人而非其中所包含的词汇内容。

早在计算机发明之前，自动语音识别的设想就已经被提上议事日程。早期的声码器可被视作语音识别及合成的雏形，其目标是将人类的语言转化为计算机可读的输入。语音识别技术的应用包括语音拨号、语音导航、室内设备控制、语音文档检索等。20 世纪 20 年代生产的“Radio Rex”玩具狗可能是最早的语音识别器，当这只狗的名字被呼唤时，它能够从底座上弹出来。

最早的基于电子计算机的语音识别系统是由 AT&T 贝尔实验室开发的 Audrey 语音识别系统，它能够识别 10 个英文数字。其识别方法是跟踪语音中的共振峰。该系统的正确率达到了 98%。

在《谍影重重 3》中，伯恩为了获得中央情报局某位探员的绝密资料，来到其办公室给他打了个电话，通过电话录音窃取了他的声音资料，然后用他的声音打开了保险箱，获取了资料。

在我国，安徽科大讯飞信息科技股份有限公司在语音合成技术、语音测试技术、语音识别技术、声纹识别技术等一系列语音交互核心技术研究及产业化方面走在世界前列，于 2011 年 12 月 29 日工业和信息化部主办的 2011 年第十一届信息产业重大技术发明评选中荣获国家信息产业最高荣誉："信息产业重大技术发明奖"。科大讯飞智能语音核心技术代表了世界的最高水平，实现了人机语音交互，使人与机器之间的沟通变得像人与人沟通一样简单。语音技术主要包括语音合成和语音识别两项关键技术。让机器说话，用的是语音合成技术；让机器听懂人说话，用的是语音识别技术。此外，语音技术还包括口语评测、语音编码、音色转换、语音消噪和增强等技术，有着广阔应用空间。

2.1.3 生物识别技术

生物识别技术（Biometric Identification Technology）是利用人体生物特征进行身份认证的一种技术。生物特征是唯一的，用于生物识别的生物特征有手形、指纹、脸形、虹膜、视网膜、脉搏、耳廓等，行为特征有签字、声音、按键力度等。基于这些特征，人们已经发展了手形识别、指纹识别、面部识别、发音识别、虹膜识别、签名识别等多种生物识别技术。图 2-3 为生物识别技术在安防、考勤系统中的应用。



图 2-3 生物识别技术应用

人类利用生物特征识别的历史可追溯到古代埃及人通过测量人体各部位的尺寸来进行身份鉴别，现代生物识别技术始于 20 世纪 70 年代中期，由于早期的识别设备比较昂贵，因而仅限于安全级别要求较高的原子能实验、生产基地等。现在由于微处理器及各种电子元器件成本不断下降，精度逐渐提高，生物识别系统逐渐应用于商业上的授权控制，如门禁、企业考勤管理系统安全认证等领域。

生物识别技术是目前最为方便和安全的识别技术，它不需要记住复杂的密码，也不需随身携带钥匙、智能卡之类的东西。由于每个人的生物特征不易伪造和假冒，所以利用生物识别技术进行身份认定，安全、可靠、准确。此外，生物识别技术产品均借助于现代计算机技术实现，很容易配合电脑和安全、监控、管理系统整合，实现自动化管理。目前人体特征识别技术市场上占有率最高的是指纹机和手形机，市场占有率分别为 34%和 26%。

经常看外国电影的人，往往会留意到里面有许多涉及高科技的情节，比如主人公要到某一



重要的场所，如实验室、机房、博物馆等，一般没有钥匙，而是通过红外探测仪，指纹、虹膜扫描，声音识别等装置确认身份，这些穿插着众多高科技元素的电影让我们眼花缭乱。

红外探测报警技术在好莱坞电影中已经屡见不鲜，如《十一罗汉》、《纵横四海》等描写神偷如何突破红外线防御体系的环节都已被打造成精彩纷呈的桥段。其中最经典躲避红外探测的电影，还是美女辛康纳利的《偷天陷阱》（见图 2-4）。

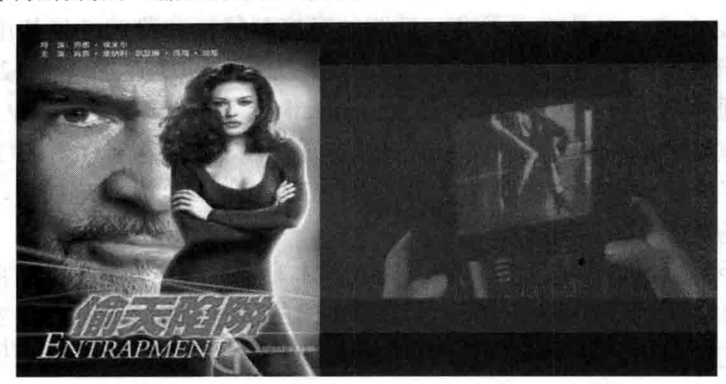


图 2-4　《偷天陷阱》剧照

1. 指纹识别技术

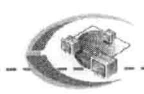
每个人包括指纹在内的皮肤纹路，在图案、断点和交叉点上各不相同，呈现唯一性且终身不变。据此，我们就可以把一个人同他的指纹对应起来，通过将他的指纹和预先保存的指纹数据进行比较，就可以验证他的真实身份，这就是指纹识别技术。

指纹识别进行身份鉴定，得益于现代电子集成制造技术和快速而可靠的计算机发展，20 世纪 60 年代，指纹自动识别系统已经开始被美国联邦调查局和法国巴黎警察局用于刑事侦破。如今，指纹识别技术已经开始走入我们的日常生活，将指纹锁应用于笔记本、机箱甚至鼠标上，可以对文件、系统起保护作用，并且进行身份识别。指纹识别系统是一个典型的模式识别系统，包括图像采集、处理、特征提取和特征比较等模块。

在电影《碟中谍》中，莎拉在杰克的帮助下，顺利地通过指纹识别系统进入了大使馆唯一的管制区（见图 2-5）。



图 2-5　电影《碟中谍》剧照



2. 虹膜识别技术

虹膜是位于眼睛的白色巩膜和黑色瞳孔之间的圆环状部分，总体上呈现一种由内向外的放射状结构，由相当复杂的纤维组织构成。虹膜包含了最丰富的纹理信息，包括很多类似于冠状、水晶体、细丝、斑点、凹点、射线、皱纹和条纹等细节特征结构，这些特征由遗传基因决定，在出生之前就确定下来，并且终身不变。虹膜的高度独特性和稳定性是其用于身份鉴别的基础。在所有生物识别技术中，虹膜识别是当前应用最为方便和精确的一种。2001 年 5 月到 10 月，受英国政府通信电子安全组 CESG（Communications Electronics Security Group）委托，英国国家物理实验室（National Physical Lab，NPL）通过广泛的实验研究，对上述各类人体生物特征识别技术作了分析比较并在实验结果中公布：虹膜识别是“最精确的”、“处理速度最快的”以及“最难伪造的”。

科幻电影《少数派报告》*中，50 年后人类就基本靠视网膜辨识身份。从商场到地铁站，在任何地方都可能被系统扫描识别。汤姆·克鲁斯饰演的预防犯罪调查科探员安德森由于受诬陷而被通缉，逃亡的过程中，安德森在无处不在的虹膜扫描下险象环生，最后他决定换眼球，希望借此逃过电子蜘蛛的虹膜扫描追踪。

2.1.4 IC 卡技术

IC 卡（Integrated Circuit Card，集成电路卡）又称集成电路卡，它是在大小和普通信用卡相同的塑料卡片上嵌置一个或多个集成电路构成的。集成电路芯片可以是存储器或微处理器。带有存储器的 IC 卡又称为记忆卡或存储卡，带有微处理器的 IC 卡又称为智能卡或智慧卡。记忆卡可以存储大量信息；智能卡则不仅具有记忆能力，而且还具有处理信息的功能。IC 卡是 1974 年一名法国新闻记者发明的。由于便于携带，存储量大，它正日益受到人们的青睐。IC 卡可以十分方便地存汽车费、电话费、地铁乘车费、食堂就餐费、公路付费以及购物旅游、贸易服务等。

IC 卡是继磁卡之后出现的又一种新型信息工具。IC 卡在有些国家和地区也称智能卡（Smart Card）、智慧卡（Intelligent Card）、微电路卡（Microcircuit Card）或微芯片卡等。它是将一个微电子芯片嵌入符合 ISO 7816 标准的卡基中，做成卡片形式，它已经十分广泛地应用于包括金融、交通、社保、校园等很多领域（见图 2-6）。



图 2-6　校园 IC 卡



按照数据读写方式，智能卡又可分为接触式 IC 卡和非接触式 IC 卡两类。

（1）接触式 IC 卡。

接触式 IC 卡由读写设备的触点和卡片上的触点相接触进行数据读写，国际标准 ISO 7816 系列对此类 IC 卡进行了规定。

（2）非接触式 IC 卡。

非接触式 IC 卡又称射频卡，成功地解决了无源（卡中无电源）和免接触这一难题，是电子器件领域的一大突破。主要用于公交、轮渡、地铁的自动收费系统，也应用在门禁管理、身份证明和电子钱包。这类卡一般用在存取频繁、使用环境恶劣的场合。国际标准也对非接触 IC 卡技术作了规范。

2.1.5　射频识别技术

射频识别技术（Radio Frequency Identification，RFID）是一项利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递并通过所传递的信息达到识别目的的技术，俗称电子标签。从信息传递的基本原理来说，射频识别技术在低频段基于变压器耦合模型（初级与次级之间的能量传递及信号传递），在高频段基于雷达探测目标的空间耦合模型（雷达发射电磁波信号碰到目标后携带目标信息返回雷达接收机）。1948 年哈里斯托克曼发表的“利用反射功率的通信”奠定了射频识别技术的理论基础。

RFID 最早出现在 20 世纪 80 年代，较其他技术明显的优点是电子标签和阅读器无须接触便可完成识别。它的出现改变了条形码依靠“有形”的一维或二维几何图案来提供信息的方式，通过芯片来提供存储在其中的数量巨大的“无形”信息。RFID 首先在欧洲市场上得以使用，最初被应用在一些无法使用条码跟踪技术的特殊工业场合（如在一些行业和公司中，这种技术被用于目标定位、身份确认及跟踪库存产品等），随后在世界范围内普及。由于射频识别技术起步较晚，至今没有制定出统一的国际标准，但是射频识别技术的推出绝不仅仅是信息容量的提升，它对于计算机自动识别技术来讲是一场革命，它所具有的强大优势会极大地提高信息的处理效率和准确度。由于 RFID 芯片的小型化和高性能芯片的实用化，射频识别标签不仅可帮助不同领域的管理者追踪物品的位置和搬运情况，还可以实时报告标签上附带的其他信息，比如温度和压力等。射频识别标签是通过连接到数据网络上的读写器来提供此类信息的，目前，射频识别标签主要作为条码的延伸而应用于工厂自动化或者库存管理等领域，但最终说来，尺寸更小的射频识别标签将应用于更广阔的领域。例如，射频识别标签可以促进网络家电的应用，家电如果拥有网络功能，使用者即使在户外也能控制它们，如可以检查冰箱中的食物，帮助使用者决定需要购买什么物品，在无线操作终端上选择食物烹饪的方式等。射频识别标签也可以应用于医院，病人身上佩戴标签，标签内含有病人的识别信息，医生和护士可以通过标签内的数据来识别病人的身份，避免认错病人，标签和读写器也能帮助医生和护士确认所使用的药物是否合适，从而避免医疗事故的发生。

RFID 产业潜力无穷，应用的范围遍及制造、物流、医疗、运输、零售、国防等方面。

2.2 RFID 技术

2.2.1 RFID 发展过程

在 20 世纪 30 年代，美国陆军和海军都面临着在陆地、海上和空中对目标的识别的问题。RFID 在历史上的首次应用是在第二次世界大战期间（约 1940 年），其当时的功能是用于分辨出敌方飞机与我方飞机。1937 年，美国海军研究试验室（U.S.Naval Research Laboratory，NRL）开发了敌我识别系统（Identification Friend-or-Foe System，IFF），将盟军的飞机和敌方的飞机区别开来。我方的飞机上装载有高耗电量的主动式卷标，当雷达发出询问的信号，这些卷标就会发出适当的响应，借以识别出自己是我军或是敌军。此系统称为 IFF。这种技术后来在 50 年代成为现代空中交通管制的基础。

早期系统组件昂贵、庞大，但随着集成电路、可编程存储器、微处理器、软件技术和编程语言的发展，创造了 RFID 技术推广和部署的基础。

20 世纪 60 年代，人类对 RFID 的探索才正式拉开了序幕。1964 年，R.F.Harrington 开始研究与 RFID 相关的电磁理论，并于 1964 年发表“Theory of Loaded Scatters”。此时商业应用也逐渐出现，如 Sensormatic、Checkpoint Systems 和 Knogo 等公司开发出了用于电子物品监控（Electronic Article Surveillance，EAS），即保证仓库、图书馆等的物品安全和监视。这种早期的商业应用被称为 1-bit 标签系统，因为它只能检测被标识的目标是否存在，从而防止物体被偷窃。标签不能携带更大的存储容量，当有多个物体存在时，甚至无法区分出被标识物体的差别。图 2-7 展示了 RFID 发展过程中里程碑式的事件。



图 2-7　RFID 发展历史（1880 —1960 年）（早期的 RFID 发展里程碑）

到了 20 世纪 70 年代末期，美国政府通过 Los Alamos 科学实验室 Koelle、Steven 和 Freyman 于 1975 年发表的“Short-Range Radio Telemetry for Electronic Identification Using Modulated Backscatter”，将 RFID 技术转移到民间。RFID 技术最先在商业上的应用是在牲畜身上，成功开发出了能够适用于特殊环境下传输距离可达 5 米的被动标签原型。



到了 20 世纪 80 年代，美国与欧洲的几家公司开始着手生产 RFID 卷标。今天来讲，RFID 技术已经被广泛应用于各个领域，从门禁管制、牲畜管理，到物流管理，皆可见到其踪迹。

在 70 年代，制造、运输、仓储等行业都试图研究和开发基于 IC 卡的 RFID 系统的应用。比如：工业自动化、动物识别、车辆跟踪等。在此期间，基于 IC 卡的标签体现出可读写、更快的速度、更远的距离等优点。但这些早期的系统仍然是专有的设计，没有相关标准，也没有功率和频率的管理。图 2-8 展示了 1960—1990 年的 RFID 发展历史。

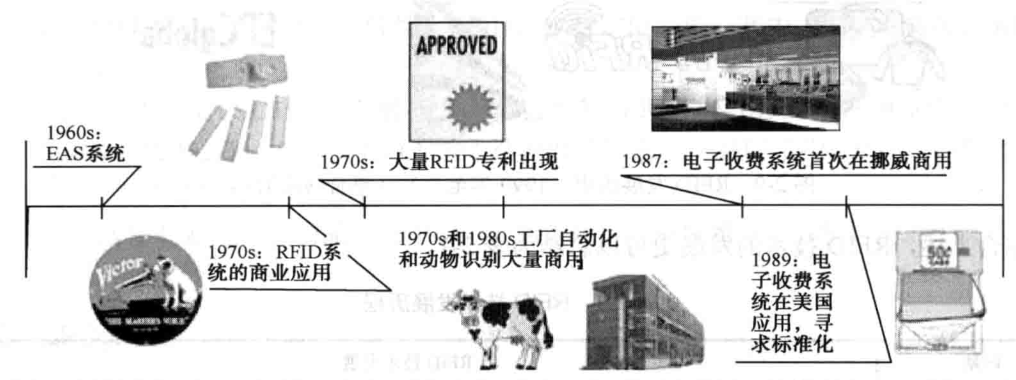


图 2-8　RFID 发展历史（1960—1990 年）（唯一性标识）

20 世纪 90 年代是 RFID 发展史上最为重要的十年，在这期间，电子收费系统在美国开始大量部署，在北美共有约 3 亿个 RFID 标签被安装在汽车尾部。1991 年，世界第一个高速公路不停车收费系统在美国俄克拉荷马州（Oklahoma）开始投入使用。1992 年，世界第一个电子收费系统和交通管理系统的集成系统在美国休斯顿安装并使用。多个地区和公司开始注意到系统之间的互操作性，即运行频率和通信协议的标准化问题。只有提供了统一的标准，RFID 才能在更广泛的领域得到应用。例如，当时 E-Zpass 系统能够兼容美国七大地区的电子收费系统，通过这套系统，附带同一个标签的汽车在七大地区均可使用。

在美国，Texas Instruments 则是这方面的推动先锋。TI 从 1991 年开始建立德州仪器注册和识别系统（Texas Instruments Registration and Identification Systems，TIRIS）。该系统如今叫 TI-RFid（Texas Instruments Radio Frequency Identification System），已经是一个主要的 RFID 应用开发平台。

在欧洲，EM Microelectronic-Marin 从 1971 年开始研究超低功率的集成电路。1982 年，Mikron Integrated Microelectronics 开始了 ASIC 技术，并在 1987 年由其奥地利分公司开始开发智能卡芯片。1995 年，Philips Semiconductors 收购了 Mikron Graz。如今 EM Microelectronic 和 Philips Semiconductors 是欧洲的主要 RFID 厂商。

从 20 世纪 90 年代末期到现在，零售巨头如 Wal-Mart、Target、Metro Group 以及一些政府机构，如美国国防部（DoD），都开始推进 RFID 应用，并要求他们的供应商也采用此技术。同时，标准化的纷争出现了多个全球性的 RFID 标准和技术联盟，主要有 EPCglobal、AIM Global、ISO/IEC、UID、IP-X 等。这些组织主要在标签技术、频率、数据标准、传输和接口协议、网络运营和管理、行业应用等方面试图达成全球统一的平台。图 2-9 展示了 1990 年至今 RFID 的

发展历史。

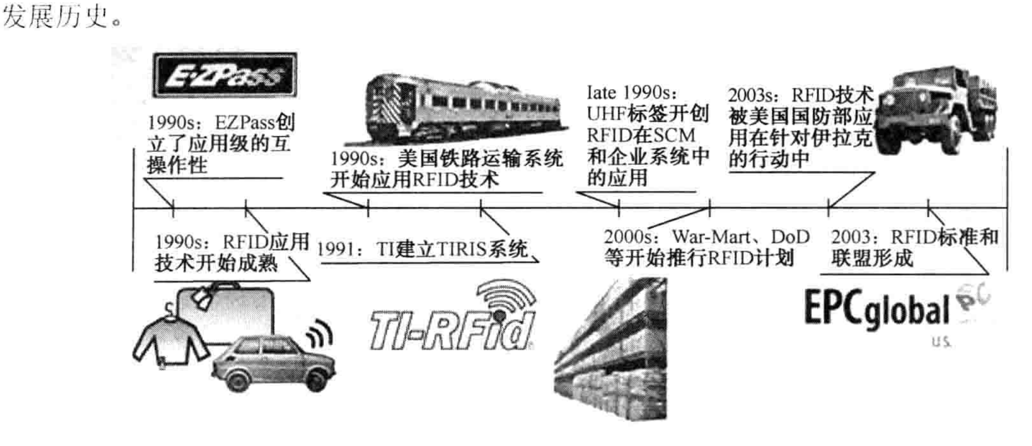


图 2-9 RFID 发展历史（1990 年至今）（整合应用开始）

综合上述，RFID 技术的发展史可以总结为表 2-1。

表 2-1 RFID 技术发展历程

时期	RFID 技术发展
1941—1950 年	雷达的改进和应用催生了 RFID 技术，1948 年奠定了 RFID 技术的理论基础
1951—1960 年	早期 RFID 技术的探索阶段，仍处于实验室实验研究
1961—1970 年	RFID 技术的理论得到进一步发展，开始了一些新的应用尝试
1971—1980 年	RFID 技术与产品研发处于一个大发展时期，各种 RFID 技术测试得到加速。出现了一些最早的 RFID 应用
1981—1990 年	RFID 技术及产品进入商业应用阶段，各种封闭系统应用开始出现
1991—2000 年	RFID 技术标准化问题日趋得到重视，RFID 产品得到广泛采用
2000 年至今	标准化问题日趋为人们所重视，RFID 产品种类更加丰富，有源电子标签、无源电子标签及半无源电子标签均得到发展，电子标签成本不断降低，应用规模迅速扩张

2.2.2 RFID 技术标准现状

目前，RFID 还未形成统一的全球化标准，市场为多种标准并存的局面，但随着全球物流行业 RFID 大规模应用的开始，RFID 标准的统一已经得到业界的广泛认同。RFID 系统主要由数据采集和后台数据库网络应用系统两大部分组成。目前已经发布或者是正在制定中的标准主要是与数据采集相关的，其中包括电子标签与读写器之间的空中接口、读写器与计算机之间的数据交换协议、RFID 标签与读写器的性能和一致性测试规范以及 RFID 标签的数据内容编码标准等。后台数据库网络应用系统目前并没有形成正式的国际标准，只有少数产业联盟制定了一些规范，现阶段还在不断演变中。

RFID 标准争夺的核心主要在 RFID 标签的数据内容编码标准这一领域。目前，形成了五大标准组织，分别代表了国际上不同团体或者国家的利益。EPCglobal 是由北美 UCC 产品统一编



码组织和欧洲EAN产品标准组织联合成立，在全球拥有上百家成员，得到了零售巨头沃尔玛，制造业巨头强生、宝洁等跨国公司的支持。而AIM、UID则代表了欧美国家和日本；IP-X的成员则以非洲、大洋洲、亚洲等国家为主。比较而言，EPCglobal 由于综合了美国和欧洲厂商，实力相对占上风。

1. ISO RFID标准

ISO负责RFID标准制定的委员会为ISO/IEC JTC1 SC31，下设5个工作组（WG1～WG5），分别涉及数据载体、数据内容、一致性、RFID、实时定位系统。其中WG4主要负责RFID技术方面的标准。

除了ISO/IEC JTC1 SC31外，其他技术委员会也参与RFID应用方面的标准制定，如TC23、TC58、TC104、TC122等。其中，ISO 11784动物射频识别——编码结构、ISO 11785动物射频识别技术概念为TC23/SC19制定。

SC31中国秘书处为中国物品编码中心，分为条码、一致性测试、射频识别三个工作组，对应其五个工作组。

2. EPCglobal

EPCglobal是由UCC和EAN联合发起的非营利性机构，全球最大的零售商沃尔玛连锁集团、英国Tesco等100多家美国和欧洲的流通企业都是EPC的成员，同时由美国IBM公司、微软、Auto-ID Lab等进行技术研究支持。此组织除发布工业标准外，还负责EPCglobal号码注册管理。EPCglobal系统是一种基于EAN • UCC编码的系统。作为产品与服务流通过程信息的代码化表示，EAN • UCC编码具有一整套涵盖了贸易流通过程各种有形或无形的产品所需的全球唯一的标识代码，包括贸易项目、物流单元、位置、资产、服务关系等标识代码。EAN • UCC标识代码随着产品或服务的产生在流通源头建立，并伴随着该产品或服务的流动贯穿全过程。EAN • UCC标识代码是固定结构、无含义、全球唯一的全数字型代码。在EPC标签信息规范1.1中采用64～96位的电子产品编码；在EPC标签2.0规范中采用96～256位的电子产品编码。

3. 日本UID

主导日本RFID标准研究与应用的组织是T-引擎论坛（T-Engine Forum），该论坛已经拥有475家成员，绝大多数都是日本的厂商，如NEC、日立、东芝等，也有少数如微软、三星、LG和SKT来自国外的著名厂商。T-引擎论坛下属的泛在识别中心（Ubiquitous ID Center-UID）成立于2002年12月，具体负责研究和推广自动识别的核心技术，即在所有的物品上植入微型芯片，组建网络进行通信。UID的核心是赋予现实世界中任何物理对象唯一的泛在识别号（Ucode）。它具备了128位（128-bit）的充裕容量，可以用128位为单元进一步扩展至256、384或512位。Ucode的最大优势是能包容现有编码体系的元编码设计，可以兼容多种编码，包括JAN、UPC、ISBN、IPv6地址，甚至电话号码。Ucode标签具有多种形式，包括条码、射频标签、智能卡、有源芯片等。泛在识别中心把标签进行分类，并设立了多个不同的认证标准。

4. 韩国

韩国通信研究院 ETRI 提出了新的基于 NID Networked-based ID 的标准化，利用存储在 RFID 电子标签、一维和二维条码中的Ⅱ号触发相关的网络信息服务。NID 的应用之一即移动 RFID 服务（Mobile RFID Service），即利用 RFID 技术、手机和无线网络开展相关服务，如公交、出租车付费等。

NID 需要一系列技术和标准的支持，包括空中接口协议、ID 方案、数据语法 OID（Object ID）、读写器控制、应用协议和内容转换等，可将目前一些主要的标准化组织联合在一起，包括 ISO/IEC JTC1 的各个分技术委员会，ITU-TJCA-NID、ITU-TSAG、ITU-TSG、ITU-CG-NID 等。

5. 中国

中国的电子标签标准工作组成立于 2005 年 10 月，受当时的信息产业部领导，下设 7 个工作组，包括总体组、标签与读写器组、频率与通信组、数据格式组、应用组、信息安全组、知识产权组。目前其工作主要处于研究阶段，已立项的 RFID 标准主要是对应 ISO 18000 系列标准。

此外，中国在食品安全追溯方面正在研究相关标准，包括：食品安全追溯方法及一般原则、食品安全追溯系统数据规范、食品安全追溯系统管理与维护规范。在集装箱方面，相关的 RFID 标准已经 ISO TC104 讨论，该标准由中集集团 CIMC 起草。目前 ISO 集装箱方面的 RFID 标准有 ISO 10374、ISO 18185、ISO 17363。由中国提出的十进制网络编码目前已引起了世界的关注。

2.2.3 RFID 系统组成与工作原理

一般来说，RFID 系统由 5 个组件组成，包括传送器（Transmitter）、接收器（Receiver）、微处理器（MicroProcessor，缩写为 μP 或 uP）、天线（Antenna）和标签（Tag）。传送器、接收器和微处理器通常都封装在一起，统称为读写器（Reader），所以人们经常将 RFID 系统分为读写器、天线和电子标签三大组件，这三大组件一般都可由不同的生产商生产。

RFID 有以下三大特点：第一，可以标识每个物体，而不像条形码是用来识别一类物体；第二，可以非接触远距离地同时对多个物体进行识读，而条形码只能在非常近的距离一个一个地识读；第三，储存的信息量非常大。

RFID 源于雷达技术，所以其工作原理和雷达极为相似。首先读写器通过天线发出电子信号，标签接收到信号后发射内部存储的标识信息，读写器再通过天线接收并识别标签发回的信息，最后读写器再将识别结果发送给主机，RFID 系统的示意图如图 2-10 所示。

其工作原理为：当标签（一般为无源标签或被动标签，Passive Tag）进入磁场后，接收读写器发出射频信号，凭借感应电流所获得的能量发送出存储在芯片中的产品信息；或者标签（有源标签或主动标签，Active Tag）主动发送某一频率的信号，读写器读取信息并解码后，送至后台管理信息系统进行数据处理。



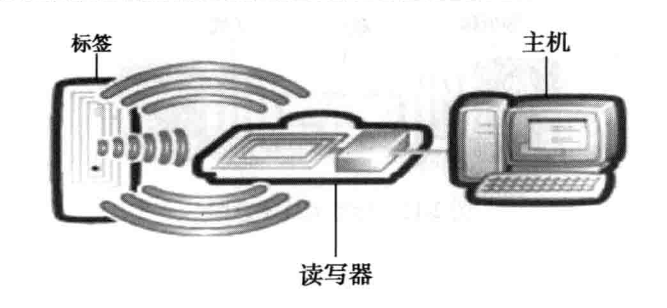


图 2-10　RFID 系统组成示意图

1. 读写器

读写器是 RFID 系统最重要的读取（或写入）标签信息的设备，也是最复杂的一个组件。因其工作模式一般是主动向标签询问标识信息，所以有时又被称为询问器（Interrogator），可设计为手持式或固定式。图 2-11 显示了几种不同外观的读写器。读写器一方面通过标准网口、RS232 串口或 USB 接口同主机相连，另一方面通过天线同 RFID 标签通信。有时为了方便，读写器和天线以及智能终端设备会集成在一起，形成可移动的手持式读写器。



图 2-11　不同外观的读写器

2. 天线

天线在标签和读写器间传递射频信号。天线同读写器相连，用于在标签和读写器之间传递射频信号。读写器可以连接一个或多个天线，每次使用时一般激活一个天线。天线的形状和大小会随着工作频率和功能的不同而不同。

RFID 系统的工作频率从低频到微波，范围很广，使得天线与标签芯片之间的匹配问题变得很复杂。图 2-12 为电子标签的天线示意图。



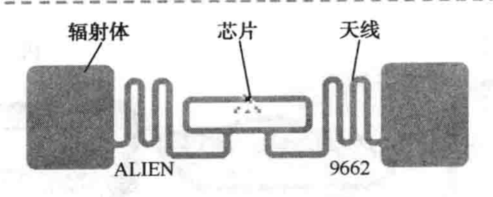


图 2-12　标签天线示意图

3. 电子标签

（1）电子标签的优点。

电子标签由耦合元件、芯片及微型天线组成，每个标签具有唯一的 RFID 编码，附着在物体上标识目标对象。图 2-13 为常见标签的外形。



图 2-13　常见标签外形

RFID 标签的原理和条形码相似，但有其特独的优点：

- 快速读写。条形码一次只能有一个条形码受到扫描；RFID 读写器可同时辨识读取数个 RFID 标签。
- 体积小且形状多样。如图 2-13 所示，RFID 标签在读取上并不受尺寸大小与形状限制，不需要为了读取精度而配合纸张的固定尺寸和印刷品质。
- 抗污染能力和耐久性。传统条形码的载体是纸张，因此容易受到污染，但 RFID 卷标是将数据存在芯片中，对水、油和化学药品等物质具有很强的抵抗性，因此可以免受污损。此外，由于条形码是附于塑料袋或外包装纸箱上，所以特别容易受到折损。
- 可重复使用。现今的条形码印刷上去之后就无法更改，RFID 标签则可以重复地新增、修改、删除 RFID 卷标内储存的数据，方便信息的更新。



- 穿透性和无屏障阅读。在被覆盖的情况下，RFID 能够穿透纸张、木材和塑料等非金属或非透明的材质，并能够进行穿透性通信。而条形码扫描机必须在近距离而且没有物体阻挡的情况下，才可以辨读条形码。
- 数据的记忆容量大。一维条形码的容量是 50Byte，二维条形码最大的容量可储存 2 至 3000 字符，RFID 最大的容量则有数兆字节（MegaByte）。随着记忆载体的发展，数据容量也有不断扩大的趋势。未来物品所需携带的资料量会越来越大，对卷标所能扩充容量的需求也相应增加。
- 数据安全性。标签内的数据通过循环冗余校验的方法来保护，使其内容不易被伪造及变造。

（2）数据存储方式。

RFID 标签采用三种方式进行数据存储：电可擦可编程只读存储器（Electrically Erasable Programmable ROM，EEPROM）、铁电随机存取存储器（Ferroelectric RAM ，FRAM）和静态随机存取存储器（Static RAM，SRAM）。一般 RFID 系统主要采用 EEPROM 方式。这种方式的缺点是写入过程中的功耗消耗很大，使用寿命一般配为 100 000 次。也有厂家采用 FRAM 方式。FRAM 的写入功耗消耗为 EEPROM 的 1/100，写入时间为 EEPROM 的 1/1000。FRAM 属于非易失类存储器。然而，FRAM 由于生产方面的问题至今未获得广泛应用。SRAM 能快速写入数据，适用于微波系统，但 SRAM 需要辅助电池不间断地供电，才能保存数据。

（3）标签分类。

- 根据是否内置电源，标签分为：

① 无源标签。标签中不含电池的标签，一般距读写器的天线的识读距离比同频段有源标签近一些，使用寿命长。

② 有源标签。标签中含有电池的标签，其距读写器的天线距离较无源标签要远，需定期更换电池。

- 根据读写方式，标签分为：

① 只读型标签。标签内容只能读出不可写入的标签称为只读型标签。

② 读写型标签。标签内容既可被读写器读出，又可由读写器写入的标签称为读写型标签。

- 根据工作频率，标签分为以下 4 种。

RFID 频率是 RFID 系统的一个很重要的指数指标，它决定了工作原理、通信距离、设备成本、天线形状和应用领域等各种因素。RFID 典型的工作频率有 125kHz、133kHz、12.56kHz、27.12MHz、433MHz、860MHz～960MHz、2.45GHz、5.8GHz 等。按工作频率的不同，RFID 系统集中在低频、高频和超高频三个区域，如图 2-14 所示。

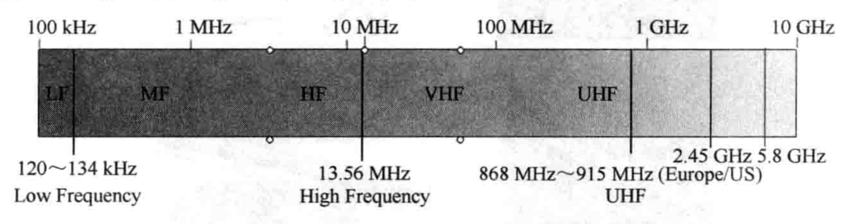


图 2-14　RFID 频率分布图

① 低频标签。工作频率在 300kHz 以下的标签称为低频标签。典型频率 125kHz、134kHz。

适用于较近距离场合门禁、一卡通。该频率主要是通过电感耦合的方式进行工作，也就是在读写器线圈和感应器线圈间存在着变压器耦合作用。通过读写器交变场的作用在感应器天线中感应的电压被整流，可作供电电压使用。磁场区域能够很好地被定义，但是场强下降得太快。一般适合于中、低频工作的近距离射频识别系统。由此可见，电磁感应系统识别距离一般较近，如图 2-15 所示。

② 高频标签。工作频率在 30MHz 以下，典型频率为 13.56MHz。在该频率的感应器不再需要线圈进行绕制，可以通过腐蚀或者印刷的方式制作天线。感应器一般通过负载调制的方式进行工作。也就是通过感应器上的负载电阻的接通和断开促使读写器天线上的电压发生变化，实现用远距离感应器对天线电压进行振幅调制。如果人们通过数据控制负载电压的接通和断开，那么这些数据就能够从感应器传输到读写器。适用于稍远距离的场合，如一卡通、会议系统等。

③ 超高频标签。工作频率为 860MHz～960MHz，通过电场来传输能量。电场的能量下降得相对较慢，但是读取的区域不是能很好地进行定义。主要是通过电磁传播或者电磁反向散射（Back Scatter）耦合（即雷达模型）方式进行实现（见图 2-16）。发射出去的电磁波，碰到目标后反射，同时携带回目标信息，依据的是电磁波的空间传播规律。电磁反向散射耦合方式一般适合于超高频、微波工作的远距离射频识别系统。由此可见，电磁传播系统识别距离较远，无源可达 10 米左右。

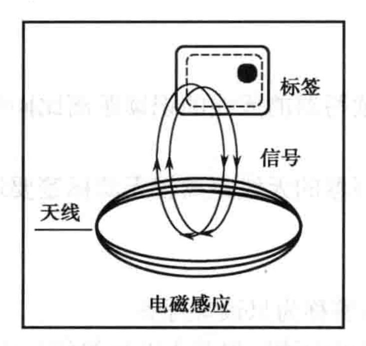


图 2-15 RFID 电磁感应通信示意图

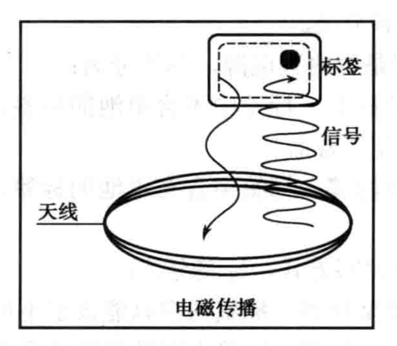


图 2-16 RFID 电磁传播通信示意图

图 2-17 为部分超高频标签，适用于较远距离场合，如物流、SCM 和车辆等。



图 2-17 UHF 标签



④ 微波标签。工作频率在1GHz以上的标签称为微波标签，典型频率为2.45GHz、5.8GHz。如集装箱自动识别用标签、高速公路不停车收费用标签、搜救、定位等，详情参见表2-2。

表2-2　根据工作频率进行电子标签分类

频　段	特　点	应　用	符合的国际标准
低频 （工作频率：125kHz～134kHz）	✧ 工作频率为120kHz～134kHz，对应波长大约为2500米 ✧ 除了金属材料影响外，一般低频能够穿过任意材料的物品而不降低它的读取距离 ✧ 工作在低频的读写器在全球没有任何特殊的许可限制 ✧ 低频产品有不同的封装形式，好的封装形式就是价格太贵，但是有10年以上的使用寿命 ✧ 虽然该频率的磁场区域下降很快，但是能够产生相对均匀的读写区域 ✧ 相对于其他频段的RFID产品，该频段数据传输速率比较慢 ✧ 感应器的价格相对于其他频段来说要贵	✧ 畜牧业的管理系统 ✧ 汽车防盗和无钥匙开门系统的应用 ✧ 马拉松赛跑系统的应用 ✧ 自动停车场收费和车辆管理系统 ✧ 自动加油系统的应用 ✧ 酒店门锁系统的应用 ✧ 门禁和安全管理系统	✧ ISO 11784 RFID畜牧业的应用——编码结构 ✧ ISO 11785 RFID畜牧业的应用——技术理论 ✧ ISO 14223-1 RFID畜牧业的应用——空中接口 ✧ ISO 14223-2 RFID畜牧业的应用——协议定义 ✧ ISO 18000-2 定义低频的物理层、防冲撞和通信协议 ✧ DIN 30745 主要是欧洲对垃圾管理应用定义的标准
高频 （工作频率：13.56MHz）	✧ 工作频率为13.56MHz，该频率的波长大概为22米 ✧ 除了金属材料外，该频率的波长可以穿过大多数的材料，但是往往会降低读取距离。感应器需要离开金属一段距离 ✧ 该频段在全球都得到认可并没有特殊的限制 ✧ 感应器一般以电子标签的形式存在 ✧ 虽然该频率的磁场区域下降很快，但是能够产生相对均匀的读写区域 ✧ 该系统具有防冲撞特性，可以同时读取多个电子标签 ✧ 可以把某些数据信息写入标签中 ✧ 数据传输速率比低频要快，价格不是很贵	✧ 图书管理系统、瓦斯钢瓶的管理应用 ✧ 服装生产线和物流系统的管理和应用 ✧ 三表预收费系统 ✧ 酒店门锁的管理和应用 ✧ 大型会议人员通道系统 ✧ 固定资产的管理系统 ✧ 医药物流系统的管理和应用 ✧ 智能货架的管理	✧ ISO/IEC 14443 近耦合IC卡，最大的读取距离为10厘米 ✧ ISO/IEC 15693 疏耦合IC卡，最大的读取距离为1米 ✧ ISO/IEC 18000-3 该标准定义了13.56MHz系统的物理层，防冲撞算法和通信协议 ✧ 13.56MHz ISM Band Class 1 定义13.56MHz符合EPC的接口定义
超高频 （工作频率：860MHz～960MHz）	✧ 欧洲和部分亚洲定义为868MHz，北美定义为902MHz～905MHz。该频段的波长大约为30厘米 ✧ 该频段功率输出目前统一的定义（美国定义为4W，欧洲定义为500mW）	✧ 供应链上的管理和应用 ✧ 生产线自动化的管理和应用 ✧ 航空包裹的管理和应用	✧ ISO/IEC 18000-6 定义了超高频RFID空中接口的物理层和通信协议；支持可读和可写操作 ✧ EPCglobal 定义了电子

续表

频　段	特　点	应　用	符合的国际标准
超高频（工作频率：860MHz～960MHz）	✧ 超高频频段的电波不能通过如水、灰尘、雾等悬浮颗粒物。相对于高频的电子标签来说，该频段的电子标签不需要和金属分开来 ✧ 电子标签的天线一般是长条和标签状。天线有线性和圆极化两种设计，满足不同应用的需求 ✧ 该频段有好的读取距离，但是对读取区域很难进行定义 ✧ 有很高的数据传输速率，在很短的时间可以读取大量的电子标签	✧ 集装箱的管理和应用 ✧ 铁路包裹的管理和应用 ✧ 后勤管理系统的应用	物品编码的结构和超高频的空气接口以及通信的协议例如：Class 0，Class 1，UHF Gen2 ✧ Ubiquitous ID 日本的组织，定义了 UID 编码结构和通信管理协议
微波（工作频率：1GHz 以上）	✧ 有源 RFID 具备了低发射功率、通信距离长、传输数据量大、可靠性高和兼容性好 ✧ 与无源 RFID 相比，有源 RFID 在技术上的优势非常明显	✧ 井下定位 ✧ 不停车收费 ✧ 港口货运管理等应用	✧ ITU-T G821（1996）、ITU-T G826（196） ✧ ITU-R E 751（1997）基于 SDH 网的无线中继系统的体系和功能概述

在将来，超高频的产品会得到大量的应用。例如 WalMart、Tesco、美国国防部（DoD）和麦德龙超市都会在它们的供应链上应用 RFID 技术。

● 根据工作方式，标签分为：

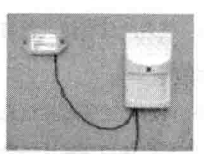
① 主动式标签。用自身的射频能量主动地发射数据给读写器，主动标签含有电源。电源设备和与其相关的电路，决定了主动式标签要比被动式标签体积大、价格昂贵。但主动式标签通信距离更远，可达上百米远。主动式标签有两种工作模式，一种是主动模式，在这种模式下标签主动向四周进行周期广播，即使没有读写器存在也会这样做；另一种为唤醒模式，为了节约电源并减小射频信号噪声，标签一开始处于低耗电量的休眠状态。读写器识别时需先广播一个唤醒命令，只有当标签接收到唤醒命令时才会开始广播自己的编码。这种低能耗的唤醒模式通常可以使主动式标签的寿命长达好几年，如 RFCode 主动标签寿命可达 7 年以上（见图 2-18）。



薄型电子标签



耐用型电子标签



干结点信号采集电子标签



被破坏时可报警的电子标签



身份卡（门卡）型电子标签



门磁电子标签

温、湿度传感器电子标签

图 2-18　RFCode 生产的电子标签



② 被动式标签。由读写器发出的信号触发后进入通信状态的标签称为被动式标签。被动式标签的通信能量从读写器发射的电磁波中获得，它既有不含电源的标签，也有含电源的标签。被动式标签的通信频率可以是高频（High Frequency，HF）或超高频（Ultra-High Frequency，UHF）。第一代被动式标签采用高频通信，其通信频段为13.56MHz。通信距离较短，最长只能到达1米左右，主要用于访问控制和非接触式付款。第二代被动式标签采用超高频通信，其通信频段为860MHz～960MHz。通信距离较长，可达3～5米，并且支持多标签识别，即读写器可同时准确识别多个标签。迄今为止，第二代被动式标签也是应用最为广泛的RFID标签，主要用于工业自动化、资产管理、货物监控、个人标识和访问控制等领域。表2-3详细地比较了这两代被动式标签。

表2-3　被动式标签相关标准

性能指标	超　高　频	高　　频
协议	EPC Class1 Gen2（ISO 18000-6C）	ISO 15693，ISO 14443
频率/MHz	860～960（区域依赖）	13.56（全球统一）
通信距离/米	3～5	1～0.1
读写器价格/USD	500～2000	100～1000
标签价格/USD	0.1～0.2	0.2～0.5
存储大小	96～1000bit	256bit～8KB
应用	供应链、自动化生成、资产管理和项目跟踪	访问控制，安全付款，验证

③ 半主动式标签。半主动式标签兼有主动式标签和被动式标签的所有优点，内部携带电源。这种标签集成传感器，可用于检测环境参数，如温度、湿度、移动性等。和主动式标签不同的是，它们通信并不需要电源提供能量，而是像被动式标签一样，通过读写器发射的电磁波获取通信能量。

（4）标签的选型。

标签是RFID应用系统的关键，它的选择和使用直接影响整个系统的性能。需要考虑几个方面的问题，首先是标签的安放位置，要考虑和读写器天线配合便于读取。第二是读写距离的要求，要设计不同的天线来满足距离要求。第三是封装形式，要考虑使用环境以及是否重复使用。第四是成本要求，因为标签的数量通常比较大，对成本比较敏感。第五是环境要求，如集装箱抗金属标签、汽车抗玻璃标签等。

4. RFID冲突

本节主要介绍RFID技术的冲突问题及分类。随着RFID技术的应用越来越广泛，RFID技术存在的问题也越发突出，其中RFID冲突问题就是其中之一。RFID系统冲突主要有标签冲突和读写器冲突。

早期的RFID系统，一次只读/写一个标签，而且标签之间要保持一定距离，确保一次只有一个标签在读写区域内，应用起来很不方便，因为很多时候不可避免地会出现多个标签进入识别区域，使得信号互相干扰，即产生冲突。冲突产生的原因有多种。

RFID 系统的冲突主要分为三种：标签冲突、读写器与读写器冲突及读写器与标签的冲突。

● 标签冲突

在 RFID 系统中，当多个标签进入到一个读写器的读写区域时就会产生冲突，冲突会导致误读、漏读。如图 2-19 所示，冲突还会导致读写器读取数据效率大大地降低，最后导致一些标签在读写器区域无法被识别。

当在一个小的区域内有多个读写器时，就会出现读写器的冲突问题，读写器的冲突又分为读写器与读写器冲突、读写器与标签冲突两种。

● 读写器与读写器冲突

当两个或多个读写器距离很近时，一个读写器会受到另外一个读写器的信号干扰。当其中一个读写器被其他读写器干扰时，读写器读取数据的效率会降低，或者出现误读的现象，这样的冲突称为读写器与读写器冲突。

如图 2-20 所示，读写器 1 会受到读写器 2 的影响，因为读写器 2 发出信号会干扰读写器 1 的判断，所以读写器 1 读取数据效率会降低，甚至误读。

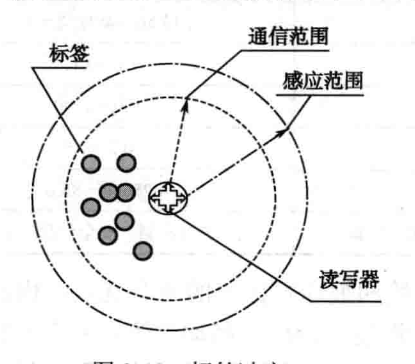


图 2-19　标签冲突

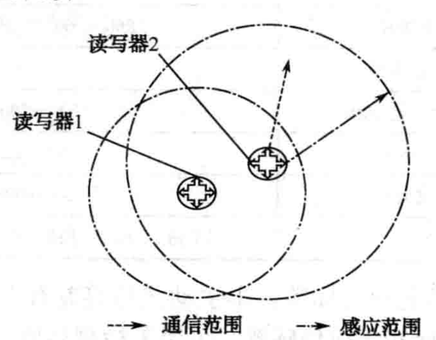


图 2-20　读写器与读写器冲突

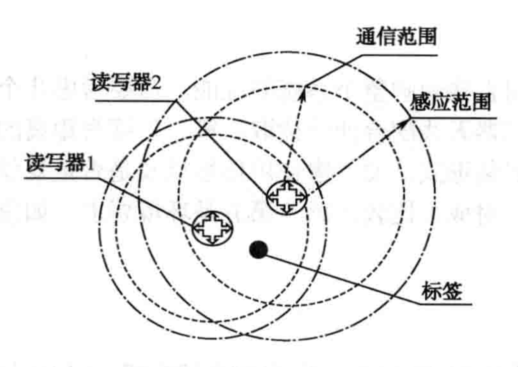


图 2-21　读写器与标签冲突

● 读写器与标签冲突

在读写器网络中，当一个或多个标签同时处于两个或多个读写器的读取范围内的话，也会出现读写器冲突的情况，这种情况称为读写器与标签的冲突。

如图 2-21 所示，有一个标签在读写器 1 与读写器 2 都可以读取的区域内，该标签会被读写器 1 和读写器 2 重复读取，或者标签无法决定发送信号给哪个读写器，从而导致读写器效率的降低，读取数据混乱。

2.2.4　阅读器到 RFID 标签的能量传输

RFID 标签依靠天线与电磁波耦合获得能量，当所处的能量场足够大时芯片即可工作。读到标签本质上包括两个要素：一是标签芯片能够获得足够的能量从而维持工作状态，并发出响



应信号，二是读写器接收到标签发出的信号并能够解析信号。类似于 A、B 两个人对话能够成功的条件是 A 讲话 B 能够听到且 B 听到后回话 A 也能够听到。目前业界读写器的接收灵敏度可以做得非常高，所以标签的最大读取距离主要依赖于标签能在多大的距离上获得足够保证芯片工作的能量。

在距离读写器为 R 的 RFID 标签处的入射波功率密度为：

$$S=\frac{P_{\mathrm{Tx}}G_{\mathrm{Tx}}}{4\pi R^2}=\frac{EIRP}{4\pi R^2}$$

其中 P_{Tx} 为读写器的发射功率；G_{Tx} 为发射天线的增益；R 是标签到阅读之间的距离；$EIRP$（等效各向同性辐射功率，Equivalent Isotropic Radiated Power）为天线有效辐射功率，指读写器发射功率和天线增益的乘积。

在 RFID 标签和发射天线最佳对准和正确极化时，RFID 标签可吸收的最大功率与入射波的功率密度 S 成正比：

$$P_{\mathrm{Tag}}=A_{\mathrm{e}}S$$

其中 $A_{\mathrm{e}}=\frac{\lambda^2}{4\pi}G_{\mathrm{Tag}}$，$G_{\mathrm{Tag}}$ 是 RFID 标签的增益。所以：

$$P_{\mathrm{Tag}}=A_{\mathrm{e}}S=\frac{\lambda^2}{4\pi}G_{\mathrm{Tag}}S=EIRPG_{\mathrm{Tag}}\left(\frac{\lambda}{4\pi R}\right)^2$$

无源射频识别系统中 RFID 标签通过读写器电磁场供电，RFID 标签功耗越大，读写距离越短，性能越差。RFID 标签是否能够正常工作也主要由 RFID 标签的工作电压来决定，这也决定了无源射频识别系统的识别距离。现代低功耗 IC 卡设计技术使 RFID 标签本身的功耗逐步降低。目前，典型的低功耗 RFID 标签工作电压在 1.2V 左右，RFID 标签本身的功耗可以低至 50μW 甚至 5μW。这使得超高频 UHF 无源 RFID 标签的识别范围在天线功率受限时仍可达到 10 米以外。射频能量辐射与范围的关系如图 2-22 所示。

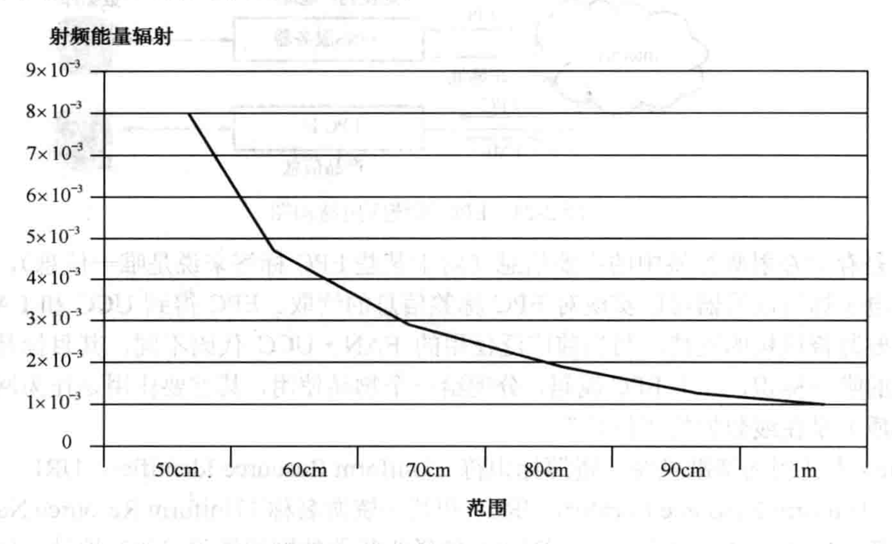


图 2-22　射频能量辐射与范围的关系

2.2.5 电子产品编码（EPC）技术

1. EPC 体系

1999 年，美国麻省理工学院 Auto-ID 中心提出 EPC 概念并研究。2003 年，国际物品编码协会（EAN/UCC）收购了 Auto-ID 中心，并成立了 EPCglobal。全球电子产品编码（Electronic Product Code，EPC）是新一代与 EAN • UCC（欧洲商品编码，European Article Numbering；美国统一代码委员会，Uniform Code Council）编码兼容的新编码，是全球统一标识系统的延伸和拓展，是物联网的核心与关键，如图 2-23 所示。



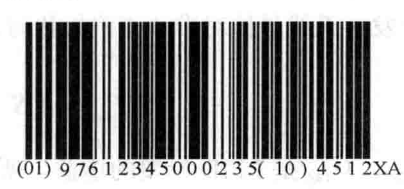


图 2-23 EAN/UPC 条码（左）与 UCC/EAN-128 条码（右）图例

基于互联网和射频识别技术的 EPC 系统，即是在计算机互联网的基础上，利用 RFID、无线数据通信等技术，构建了一个实现全球物品信息实时共享的物联网。它将成为继条形码技术之后，再次变革商品零售结算、物流配送及产品跟踪管理模式的一项新技术，如图 2-24 所示。

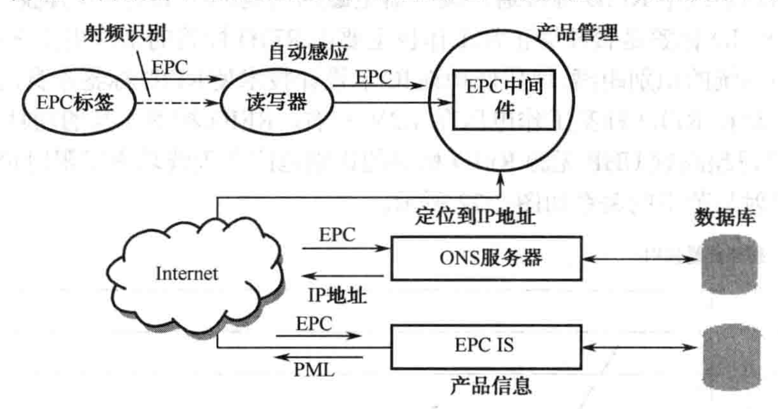


图 2-24 EPC 系统应用结构图

EPC 是存储在射频标签中的主要信息（对于某些 EPC 标签来说是唯一信息），通过射频识别系统的电子标签读写器可以实现对 EPC 标签信息的读取。EPC 得到 UCC 和 EAN 两个国际标准的主要监督机构的支持，与当前广泛使用的 EAN • UCC 代码不同，其目标是提供对物理世界对象的唯一标识，一个 EPC 编码，分配给一个物品使用，其首要作用是作为网络信息的参考，其本质上是在线数据的“指针”。

Internet 中使用的基准是统一资源标识符（Uniform Resource Identifier，URI），包括统一资源定位符（Uniform Resource Locator，URL）和统一资源名称（Uniform Resource Name，URN），由域名服务（Domain Name Service，DNS）翻译为相关的网络协议（IP）地址，即网络信息的



地址。同样，Auto-ID 中心提供的对象名称解析服务（ONS）直接将 EPC 编码翻译成 IP 地址，IP 地址对应的主机储存相关的产品信息。

为了实现上述功能，EPC 编码需要满足如下几个特殊的规定和要求。首先，必须有足够多的 EPC 编码来满足过去、现在和未来对物品标识的需要，即必须考虑所有物理对象的数量，具体字节的分配情况如表 2-4 所示。从世界人口总数（大约 60 亿）到大米总粒数（粗略估计 1 亿亿粒），EPC 必须有足够大的地址空间来标识所有这些对象。现在 EPC 标签的编码应用较多的主要有 64 位、96 位及 256 位三种，具体结构如表 2-5 所示。其次，必须保证 EPC 编码分配的唯一性并寻求解决编码冲突的方法。这就产生了由谁或什么组织负责 EPC 编码的分配问题。除了组织管理和立法机关的管理，EPC 命名空间的创建和管理可以借助于自动化软件。当然，还存在 EPC 码的使用期限和再利用问题。某些组织可能需要不定期地跟踪某一产品，就不能对该产品重新分配 EPC 码。至少希望在可预见的将来，对特殊的产品，将有一个唯一永久标识。

表 2-4　具体字节的分配情况

比　特　数	唯一编码数	对　象
23	6.0*106/年	汽车
29	5.6*108 使用中	计算机
33	6.0*109	人口
34	2.0*1010/年	剃刀刀片
54	1.3*1016/年	大米粒数

表 2-5　EPC-96/256 位编码结构

EPC-96 位编码结构				
	标头	厂商识别代码	对象分类代码	序列号
EPC-96	8	28	24	36
EPC-256 位编码结构				
EPC-256	标头	厂商识别代码	对象分类代码	序列号
	8	32	56	160
	8	64	56	128
	8	128	56	64

2. EPC 特性

EPC 编码具有如表 2-6 所示的特性。

表 2-6　EPC 特性

特　性	描　述
科学性	结构明确，易于使用、维护
兼容性	EPC 编码标准与目前广泛应用的 EAN・UCC 编码标准是兼容的，目前广泛使用的 GTIN、SSCC、GLN 等都可以顺利转换到 EPC 中去

续表

特　性	描　述
全面性	可在生产、流通、存储、结算、跟踪、召回等供应链的各环节全面应用
合理性	由 EPCglobal、各国 EPC 管理机构（中国的管理机构称为 EPCglobal China）、被标识物品的管理者分段管理、共同维护、统一应用，具有合理性
国际性	不以具体国家、企业为核心，编码标准全球协商一致，具有国际性

3. EPC 的 GEN X 协议

（1）EPC 的 Gen1 协议。

Gen1 标准是 EPCglobal 的前身 Auto-IDCenter 制定的。EPC 的 Gen1 是第一代之意，Gen 是 generation（世代）的缩写。它支持 Class0 标签和 Class1 标签，其中 Class0 标签是只读的，不可以写入；而 Class1 标签虽是可读写的，但是只能写一次，写完后就成为只读标签，这两种标签都不具有保密性。

（2）EPC 的 Gen2 协议。

因 Gen1 存在安全问题等多个缺陷，EPCglobal 在 Gen1 颁布不久便立即开始制定新的标准协议 Gen2。Gen2 是 EPCglobal 制定的 Class1UHF 频段射频识别空中接口的第二代标准。在 Gen2 协议下的标签可以重复读写，并且增加了保密性能。此后 EPCglobal 和国际标准化组织合作，以该标准为基础出台了 ISO 18000-6C 国际标准。

目前几乎所有的标签厂商已停止了 Gen1 协议的超高频芯片的开发和生产，超高频领域市场上主流产品均为符合 C1G2 协议产品。

（3）Gen2 协议特点。

Gen2 协议具有如表 2-7 所示的特点。

表 2-7　Gen2 协议的特点

特　点	描　述
兼容性	C1G2 标准适用谱较宽（860MHz～960MHz），符合各国 UHF 频段的规范，保证了不同生产商的设备之间具有良好的兼容性，也保证了 EPCglobal 网络系统中的不同组件之间的协调工作
开放性	C1G2 标准对 EPCglobal 成员和签订了 EPCglobal IP 协议的单位免收专利费。在标准的制定过程中，BTG、Alien 和 Matrices 等 60 余家 RFID 公司签署了 EPCglobal 无特权许可协议，鼓励 C1G2 标准的免版税使用，有利于 RFID 产品的市场推广
安全性	C1G2 标准在芯片中具有特定的口令，可以有效地防止芯片被非法读取。C1G2 采用简单的两个 32 位的密码。一个密码（access password）用来控制标签的读写权，在读写器与标签的通信中采用加密保证；另一个密码（kill password）用来控制标签的销毁权，采用“灭活”的方式（kill），即当标签收到读写器的有效灭活指令后，标签自行永久销毁
可靠性	标签具有高识别率，在较远的距离测试具有近 100%的读取率；容许标签延时后进入识读区仍能被读取，这是 Gen1 标签所不能达到的；抗干扰性强，更广泛的频谱与射频分布提高了 UHF 的频率调制性能，减少了与其他无线设备之间的干扰

续表

特 点	描 述
读取速度	C1G2 标准采用基于 Aloha 防碰撞算法，能快速适应标签数量的变化，在阅读批量标签时能避免重复阅读。其读取速度是第一代 EPC 标准的 10 倍，能够满足高速自动作业和大批量标签阅读应用场合
实用性	C1G2 标签的芯片尺寸可以缩小到现有版本的一半到三分之一，降低了 RFID 标签的制造成本。标签的存储能力也得到了增加，芯片中有 96 字节的存储空间，可满足各种 RFID 应用对数据存储的需要
无线接口	C1G2 标准采用了适合标签工作的数据编码和调制方式，即下行链路（读写器到标签）采用 PIE（Pulse-Interval Encoding）编码的 ASK 调制，上行链路（标签到读写器）采用 Miller 编码的副载波调制或 FM0 编码的 ASK 调制。 C1G2 空中接口协议位于 EPCglobal 协议簇架构框架底层，协议规定了标签和读写器的接口，扮演着 RFID 射频通信基础角色。 C1G2 物理层包括前向信道和反向信道两个部分。首先读写器向标签发出经 DSB-ASK、SSB-ASK 或 PR-ASK 调制的信息，标签通过反向散射调制该载波的幅度或相位来向读写器返回信息，标签—读写器通信的过程是半双工的

（4）EPCGen2 协议的发展。

Auto-IDCenter 的目标是规范编码系统和网络构造，并且采用 ISO 协议作为空中接口标准。早期，EAN 和 UCC 致力于制作符合 ISO 的 UHF 协议的全球标签（GTAG）的标准。但是，Auto-IDCenter 反对这样做，原因在于 ISO 中的 UHF 协议过于复杂，并且因此导致电子标签的成本居高不下。

Auto-IDCenter 于是独自开发 UHF 协议，最初计划制定一套适用于不同级别标签的协议。级别越高的标签越完善。结果却一直在调整计划。最终，Auto-IDCenter 采用 Class0 和 Class1 的两种不同的协议，这意味着终端用户必须购买不同的读写器来读取 Class1 和 Class0 的标签。

2003 年，Auto-IDCenter 的 EPC 技术因得到了 UCC 的认可，而开始与 EAN 组织进行合作，使 EPC 技术商业化。2003 年 11 月，Auto-IDCenter 运作成立 EPCglobal，并将 Class0 和 Class1 协议转交给 EPCglobal 进行后续工作。后来 EPCglobal 通过会议批准 Class0 和 Class1 协议作为 EPC 第一代标准，一般称为 Gen1 协议。

Gen1 协议有两个缺点，其一是 Class0 和 Class1 协议互不兼容，并且与 ISO 不兼容。其二是它们不能做到全球通用，例如，Class0 发射信号时使用一种频率，而接收信号时用另一种不同频率，这也不符合欧洲的标准。

2004 年，EPCglobal 开始着手第二代协议（Gen2）的开发，与 Gen1 不同，这个协议使得 EPC 标准将更加接近 ISO 标准。2004 年 12 月，EPCglobal 又通过了 Gen2。这样 Gen2 和 ISO 标准同时成为 RFID 产品厂家的标准。

Gen2 虽然接近了 ISO，但是，关于 AFI 却与 ISO 不同。大部分的 ISO 标准都有 AFI，这是一个 8bit 的编码，用来识别标签源码，来防止 EPCglobal 对标准的垄断。但是，生产商已经开始用 Gen2 标准来生产产品，这将在供应链中形成全球使用 Gen2 的趋势。

EPC 的 Gen2 标准于 2006 年 3 月得到 ISO 的批准认可，纳入 ISO 标准体系；对应标准为 ISO 18000-6C。

4. EPC 标签的通用标识符

EPC 标签编码的通用结构是一个二进制比特串，由一个分层次、可变长度的标头以及一系列数字字段组成（见图 2-25），码的总长、结构和功能完全由标头的值决定。标头具有可变长度，如 2 位和 8 位，2 位的标头有 3 个可能性的值（01、10 和 11），8 位标头有 63 个可能的值（标头前两位必须是 00，而 00000000 保留，以允许使用长度大于 8 位的标头）。标签长度可以通过检查标头最左（或称为“引导头”）的几位进行识别，而引导头的理想值为 1 位（最好不要超过 2 位或 3 位），使 RFID 读写器可以很容易确定标签长度。

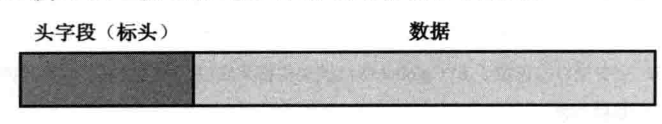


图 2-25 EPC 的一般形式

EPC 标签数据定义的编码方案标头如表 2-8 所示。若当前已分配的标头前两位非 00 或前 5 位为 00001，则可以推断该标签是 64 位；否则标头指示此标签为 96 位。

表 2-8 电子产品编码

标头（二进制）	标签长度/位	EPC 编码方案
01	64	[64-位保留方案]
10	64	SGTIN-64
11	64	[64-位保留方案]
0000 0001	Na	[1-位保留方案]
0000 001x	Na	[2-位保留方案]
0000 01xx	Na	[4-位保留方案]
0000 1000	64	SGTIN-64
0000 1001	64	SLN-64
0000 1010	64	GRAI-64
0000 1011	64	GIAI-64
0000 1010 0000 1111	64	[4 个 64-位保留方案]
0001 000 …… 0010 1111	Na	[32 个保留方案]
0011 0000	96	SGTIN-96
0011 0001	96	SSCC-96
0011 0010	96	GLN-96
0011 0011	96	GRAI-96
0011 0100	96	GIAI-96

续表

标头（二进制）	标签长度/位	EPC 编码方案
0011 0101	96	GID-96
0011 0110 …… 0011 1111	96	[10 个 96-位保留方案]
0000 0000		[为未来头字段长度大于 8 位保留]

EPC 标签数据标准定义了一种通用的标识类型，即 GID-96（General Identifier，通用标识符），它不依赖任何已知的现有规范或标识方案。此标识由 4 个字段组成：通用管理者代码、对象分类代码、序列代码以及标头，标头保证 EPC 命名空间的唯一性，如表 2-9 所示。

表 2-9 通用标识符（GID-96）

	标　头	通用管理者代码	对象分类代码	序列代码
GID-96	8	28	24	36
	0011 0101 （二进制值）	268 345 456 （十进制容量）	16 777 216 （十进制容量）	68 719 476 736 （十进制容量）

通用管理者代码标识一个组织实体（本质上一个公司管理者或其他管理者），负责维持后继字段的编号、对象分类代码和序列代码。EPCglobal 分配通用管理者代码给实体，确保每一个通用管理者代码是唯一的。对象分类代码用于识别一个物品的种类或“类型”，且在每一个通用管理者代码之下必须是唯一的。例如，消费者包装品（Consumer Packaged Goods，CPG）的库存单元（Stock Keeping Unit，SKU）或高速公路系统的不同结构，比如交通标志、灯具和桥梁等，这些产品的管理实体为一个国家。最后，序列代码在每一个对象分类代码之下是唯一的。换句话说，管理实体负责为每一个对象分类代码分配唯一的、不重复的序列代码。

2.3 实训

2.3.1 实训一：实验箱安装与连接

1. 任务目标

（1）熟悉 RFID 实验箱硬件结构。
（2）掌握 RFID 硬件设备与计算机通过串口进行链接。
（3）了解 RFID 读写器的主要功能模块。
（4）搭建 RFID 读写器。
（5）熟悉 RFID 设备基本硬件。

2. 设备准备

（1）RFID 实验箱。

（2）计算机一台。

3. 任务实施

步骤 1：了解实验箱的构造。打开 RFID 实验箱，实验箱的构造如图 2-26～图 2-31 所示。其中图 2-27 为超高频模块，图 2-28 表示高频和低频模块及天线，图 2-29 表示开关，从左至右分别是超高频、低频、高频跳线帽，拔掉跳线帽该路会被关闭；实验箱正常使用时应当将三个跳线帽同时安装好；实验箱控制软件能够智能选择所需要的读写器模块。连接线如图 2-30 所示，图 2-31 中白色部分是天线。

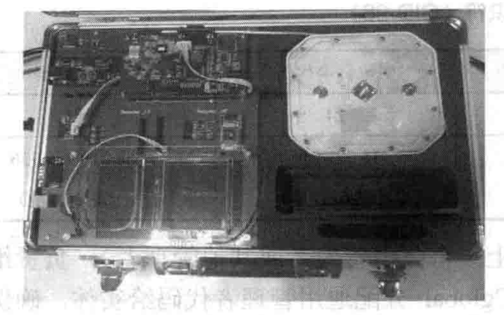


图 2-26　RFID 实验箱

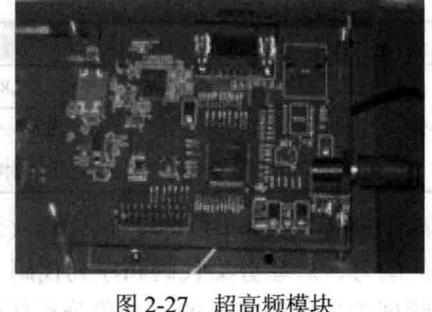


图 2-27　超高频模块

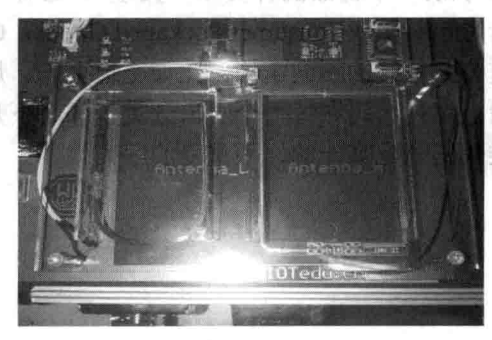


图 2-28　高频和低频模块

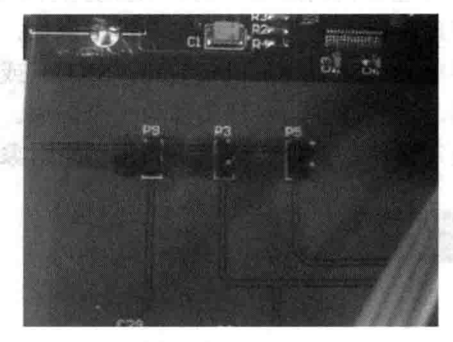


图 2-29　开关

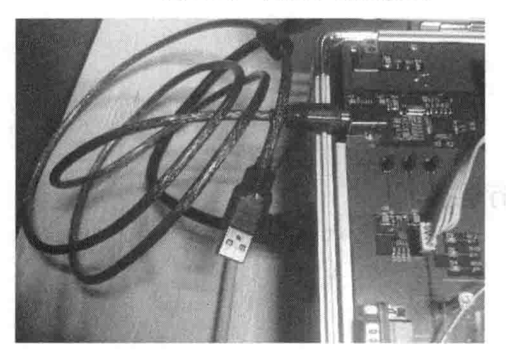


图 2-30　连接线



图 2-31　天线



步骤 2：开关电源。开机时待所有连接线连接完毕时打开电源开关，关机时先关闭计算机上的应用软件，关闭电源开关后再断开相关连接线。

步骤 3：如图 2-32 所示连接 USB 转串口线。打开电源，实验箱上电后指示灯如图 2-33 所示。然后，安装 USB 转串口驱动程序，双击 CDM20814_Setup.exe，进行安装，界面如图 2-34 所示。

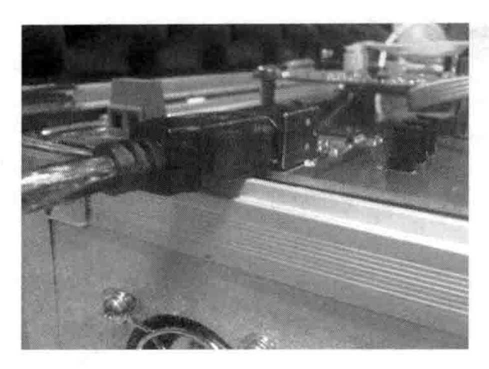




图 2-32　USB 转串口线

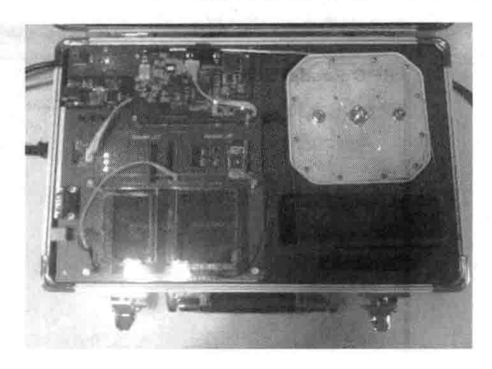


图 2-33　上电后效果

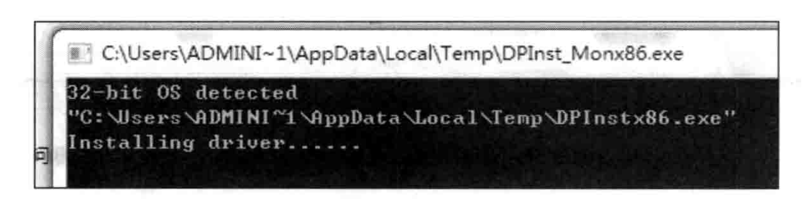


图 2-34　安装 USB 转串口驱动程序界面

USB 转串口安装成功后，右击“我的电脑”，在弹出的窗口中单击“设备管理器”，查看“端口”，显示如图 2-35 所示的可用串口号，出现 4 个 USB Serial Port，编号最小的串口（COM7）用于超高频读写器，编号最大的串口用于高频读写器（COM10），编号第二大的串口（COM9）用于低频读写器，另外剩余一路串口没有使用（COM8）。

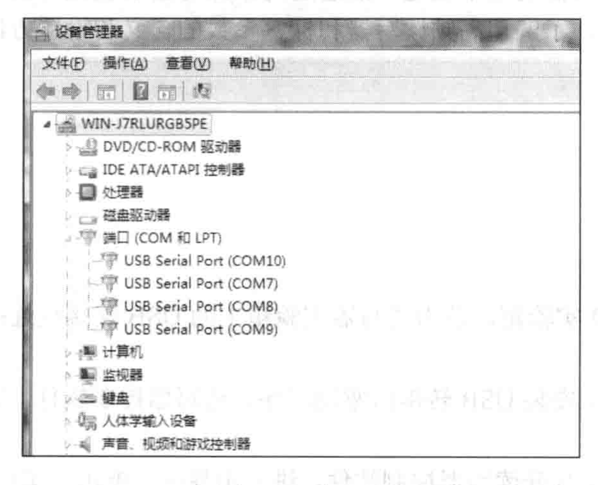


图 2-35　串口号

一般情况下，实验箱控制软件中加载读写器时，（Add LF/HF/UHF Reader）软件能够根据所选择的读写器类型智能选择对应的串口，在后续弹出的串口下拉式选项中显示的端口就是正确的端口。总之，实验箱使用跳线帽时，端口选择均无须配置，选择默认设置即可。

本实验箱控制软件为绿色版，无须安装，双击.exe 文件运行即可，初始界面如图 2-36 所示。接下来，即可进行实验箱的操作了。

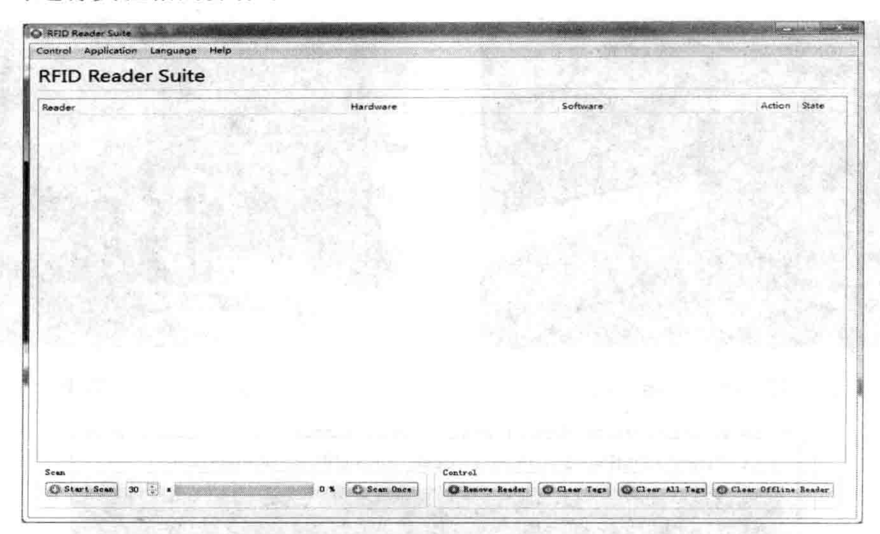


图 2-36　RFID Reader 控制软件界面

2.3.2　实训二：超高频读写器的基本认知

1. 任务目标

（1）了解超高频读写器的基本设置，熟悉超高频读写器的设置与使用。

（2）通过本次实训，了解超高频读写器和标签参数的含义和设置方法。

2. 设备准备

（1）RFID 实验箱。

（2）计算机一台。

3. 任务实施

步骤 1：打开 RFID 实验箱，使用读写器实验箱上的 USB 连接线连接实验箱和计算机，启动电源。

步骤 2：在计算机上安装 USB 转串口驱动程序、读写器控制软件。安装方法见实验箱软件安装文档。

步骤 3：在计算机上打开读写器控制软件，进入主界面，单击主菜单“Control”，选择下拉



菜单中“Add UHF Reader”选项，如图 2-37 所示。

步骤 4：选择串口（弹出的显示值即对应串口），如图 2-38 所示，单击“OK”按钮，进入如图 2-39 所示的超高频读写器选择界面。主界面上显示读写器基本信息，选中该读写器，右击选中“Reader Settings and Diagnostics”选项，然后进入读写器参数设置界面，如图 2-40 和图 2-41 所示。

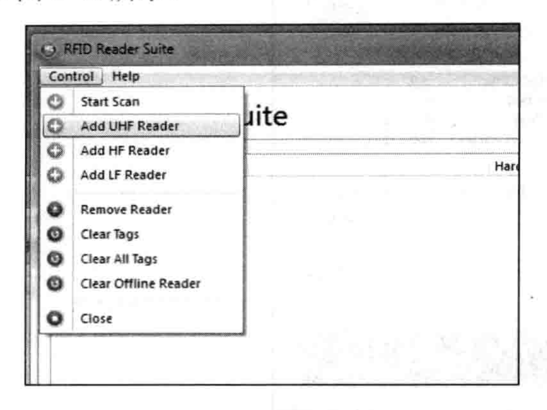


图 2-37　读写器控制软件界面

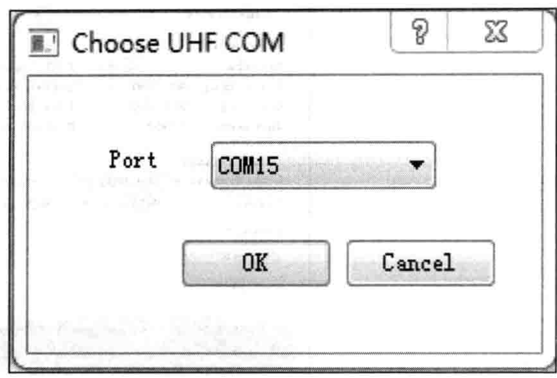


图 2-38　串口选择窗口

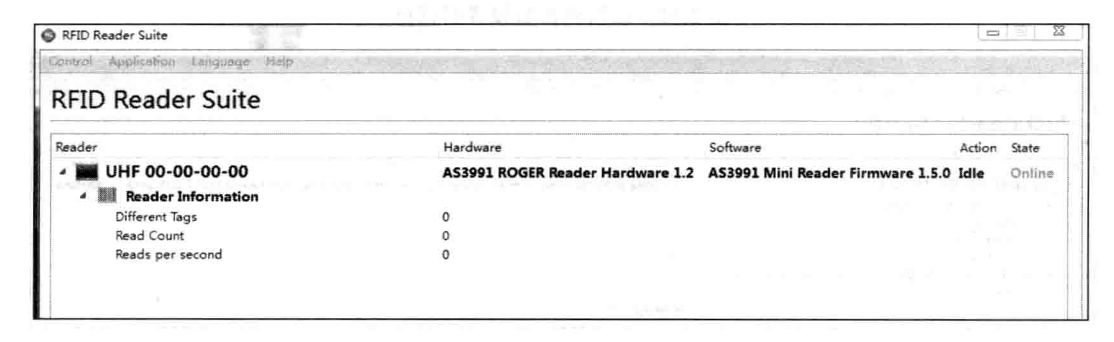


图 2-39　超高频读写器选择

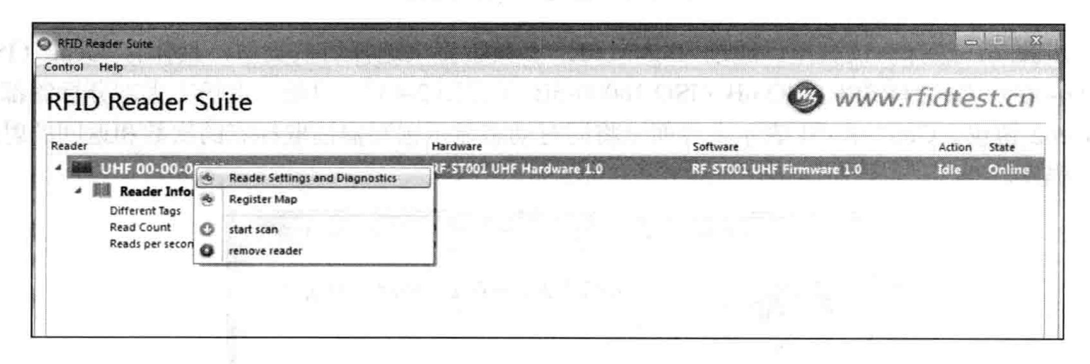


图 2-40　选择读写器参数

步骤 5：设置读写器读取标签的频率。Inventory Delay 参数用来设置读写器读取标签的频率，例如：其值设置为 10ms，表示读写器每间隔 10ms 读取一次标签信息。读写器读取标签的次数在主界面上实时动态显示，如图 2-42 所示。

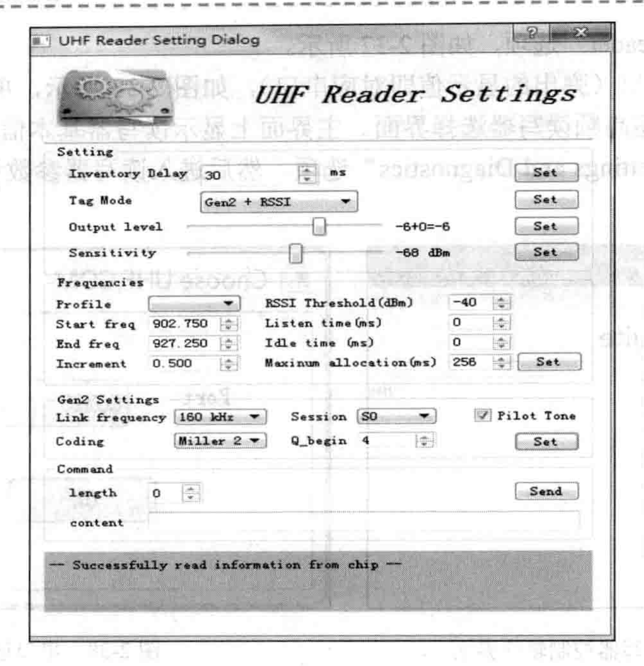


图 2-41　读写器参数设置对话框

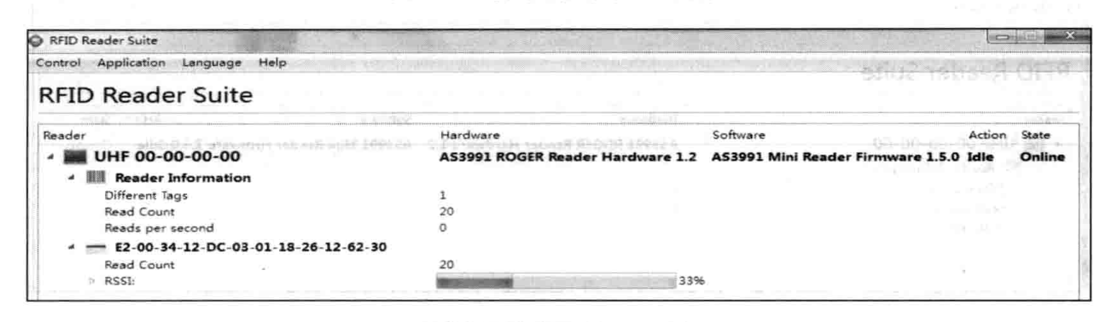


图 2-42　读取频率设置界面

步骤 6：选择协议类型。通过 Tag Model 参数设置来选择协议类型，具体有 Gen2（ISO 18000-6C）、Gen2+RSSI、ISO 6B（ISO 18000-6B）（见图 2-43）。目前，市场上大部分标签都遵守 Gen2 协议。Gen2+RSSI 表示主界面上将同时动态显示读写器读取标签的次数和返回的射频信号强度。

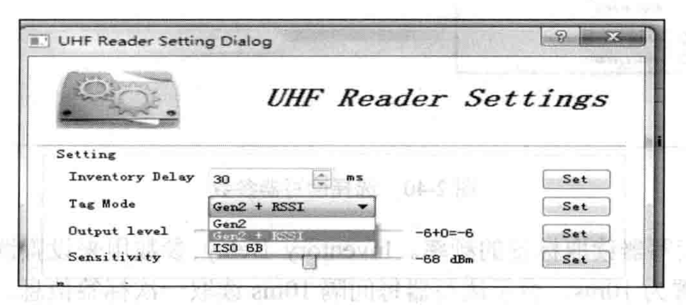
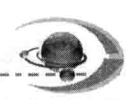


图 2-43　协议选择界面



步骤 7：读写器读取功率和灵敏度设置。Output level 参数和 Sensitivity 参数分别用于调节读写器读取功率和灵敏度。功率设置值越大，读写器读取标签的有效距离越长；灵敏度设置值越小，读写器读取标签的灵敏度越高。

Frequencies 中有 8 项参数，图 2-44 显示的 Profile 参数表示全球不同国家和地区对 UHF 频段设置的不同标准，包括 USA、Europe、Japan、Chin***.625、Chin***.125、Korea 等，一旦选择某一标准，其余的 7 项参数也随即确定。当然，在理解了各项参数实际功用和意义后，也可对这些参数进行自定义设置。Gen2 Settings 中的 4 项参数是对协议本身进行参数的设定，此项内容设置方法可以参考 ISO 18000-6C 协议等资料。

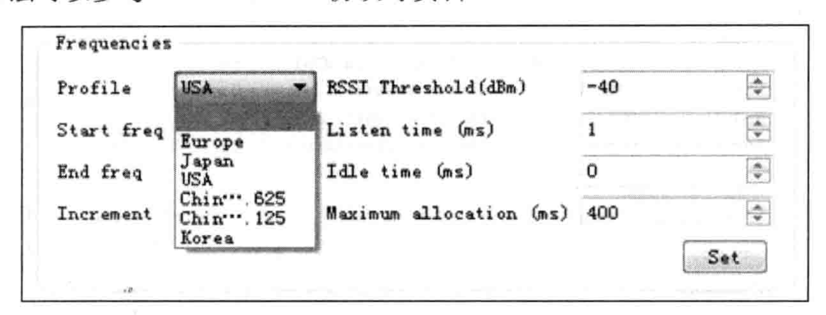


图 2-44　功率与频率设置界面

2.3.3　实训三：Gen2 协议下标签读写

1. 任务目标

熟悉 Gen2 协议标签数据的读取和写入过程。通过读写器控制软件控制 RFID 读写器对超高频 RFID 标签进行读取操作，同时对 EPC 数据进行改写操作。

2. 设备准备

（1）RFID 实验箱。
（2）计算机一台。
（3）超高频 RFID 标签一只。

3. 任务实施

步骤 1：启动读写器。打开 RFID 实验箱，连接好实验箱和计算机，将超高频天线固定在超高频读写器的天线端口上，开启电源。

步骤 2：放置标签。取一只标签，放置在超高频读写器天线上。

步骤 3：系统设置。打开读写器控制软件，设置好读写器的相关的参数（见图 2-45）。

步骤 4：读取标签。主界面上显示读写器基本信息，选中该读写器，右击、单击 Start scan 则开始读取标签，如图 2-46 所示。然后单击图中的标签号，弹出标签参数设置窗口，该窗口可针对标签进行操作，如图 2-47 所示。

UHF Reader Setting Dialog

UHF Reader Settings

Setting
Inventory Delay 30 ms Set
Tag Mode Gen2 + RSSI Set
Output level -6+0=-6 Set
Sensitivity -68 dBm Set

Frequencies
Profile
Start freq 902.750
End freq 927.250
Increment 0.500
RSSI Threshold(dBm) -40
Listen time(ms) 0
Idle time (ms) 0
Maxinum allocation(ms) 256 Set

Gen2 Settings
Link frequency 160 kHz
Coding Miller 2
Session S0
Q_begin 4
Pilot Tone
Set

Command
length 0 Send
content

-- Successfully read information from chip --

图 2-45　读写器参数设置界面

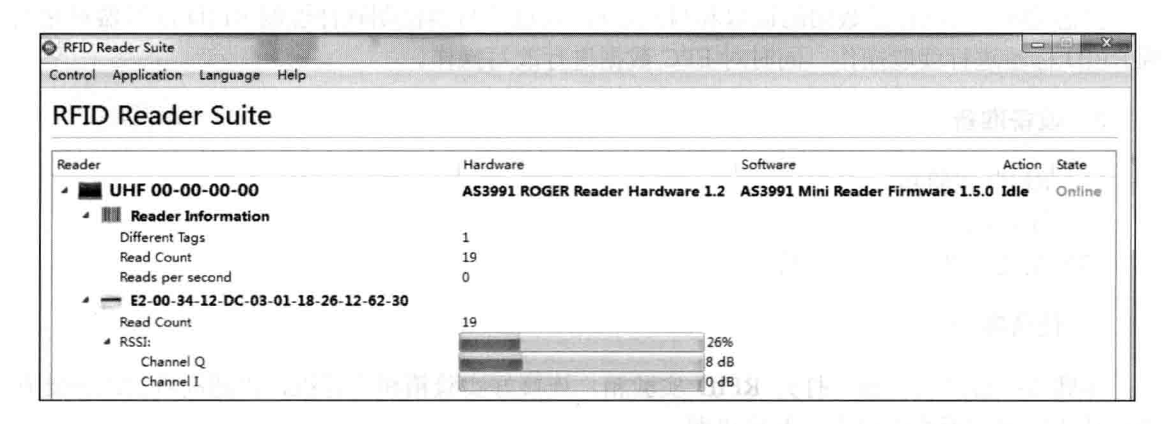


图 2-46　读取标签信息

步骤 5：修改标签 EPC 信息。在图 2-47 界面上单击“Set EPC”按钮，出现 EPC 修改界面，如图 2-48 所示，输入 EPC 长度和新的 EPC，单击“OK”按钮。



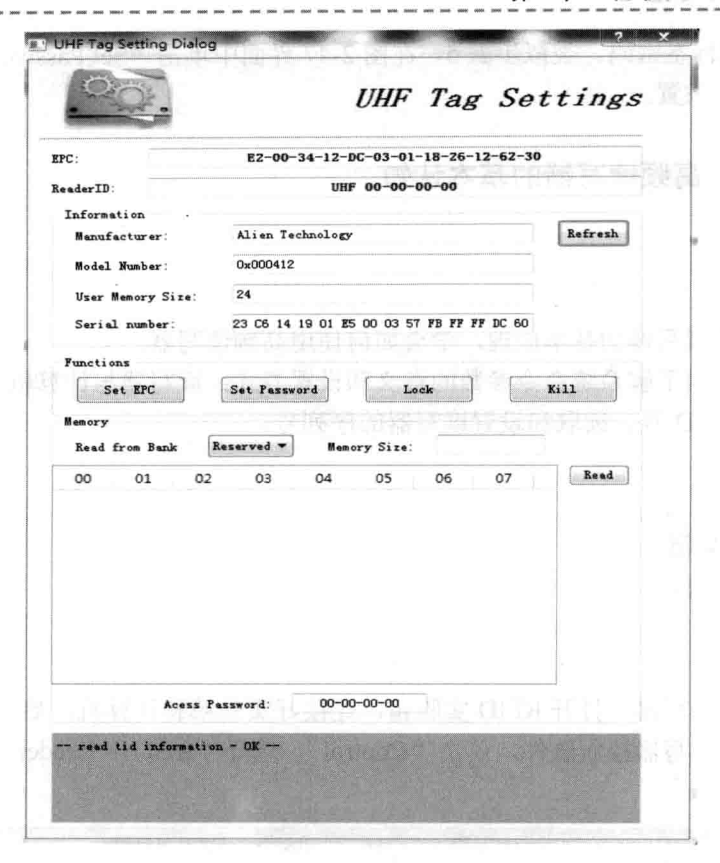


图 2-47　超高频标签设置

图 2-48　EPC 设置

步骤 6：设置标签密码。类似步骤 5，在图 2-47 界面中单击“Set Password”按钮，可对标签的访问密码进行设置。

2.3.4 实训四：高频读写器的基本认知

1. 任务目标

（1）了解高频读写器的基本原理，学会如何使用高频读写器。

（2）通过本实训了解系统命令参数的意义和设置方式：读写器与计算机通信的波特率、读取和设置读写器的 ID 号、读取和设置读写器的序列号。

2. 设备准备

（1）RFID 实验箱。

（2）计算机一台。

3. 任务实施

步骤 1：启动读写器。打开 RFID 实验箱，连接好实验箱和计算机，启动电源。

步骤 2：打开读写器控制软件，单击“Control”，选择“Add HF Reader”，加载高频模块，如图 2-49 所示。

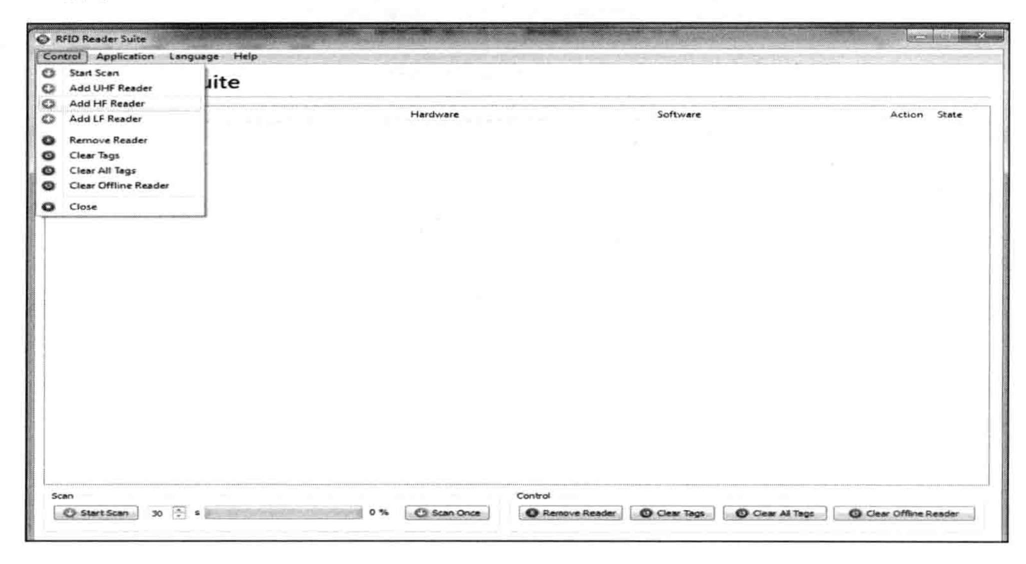
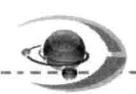


图 2-49　读写器控制软件

步骤 3：在弹出的窗口中选择高频模块对应的串口、波特率。弹出窗口默认显示的 COM 口即是高频模块对应的串口，这里为 COM7（见图 2-50），波特率选项分别是 9600 波特、19200 波特、38400 波特、57600 波特和 11520 波特。选择 9600 波特，单击“OK”按钮，进入高频读写器界面，如图 2-51 所示。



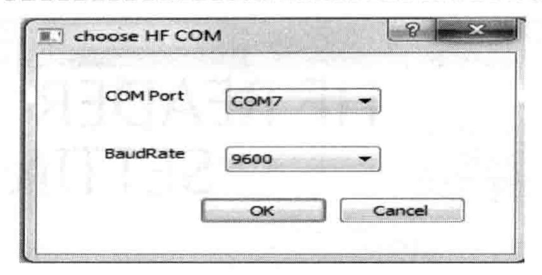


图 2-50　串口、波特率的选择

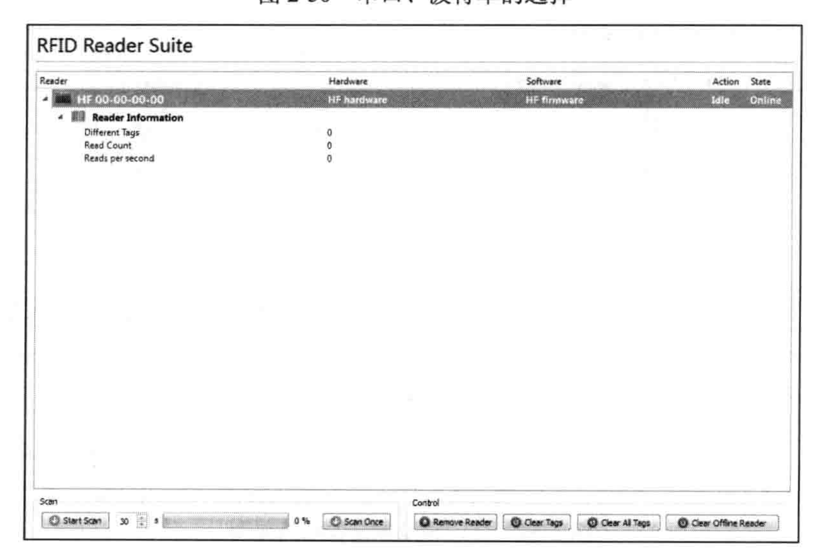


图 2-51　高频读写器界面

步骤 4: 单击 HF 读写器，右击，在弹出的界面中选择第一项 Reader Settings and Diagnostics，进入高频读写器设置界面，如图 2-52 和图 2-53 所示。

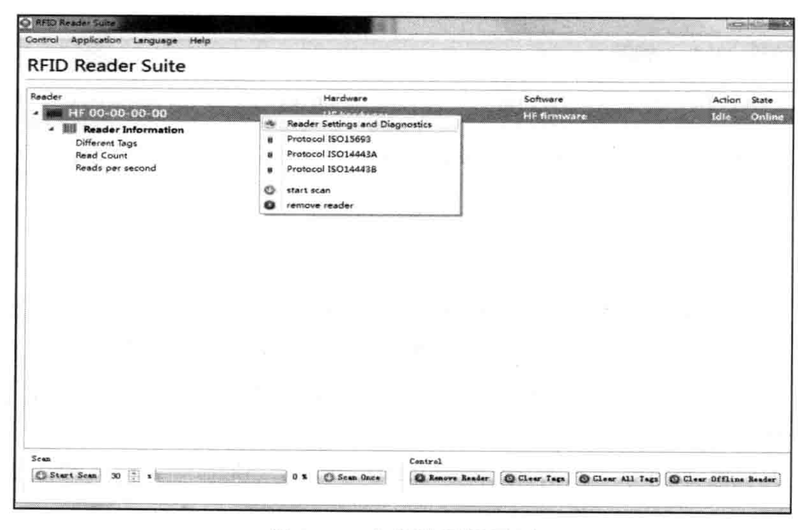


图 2-52　高频读写器界面

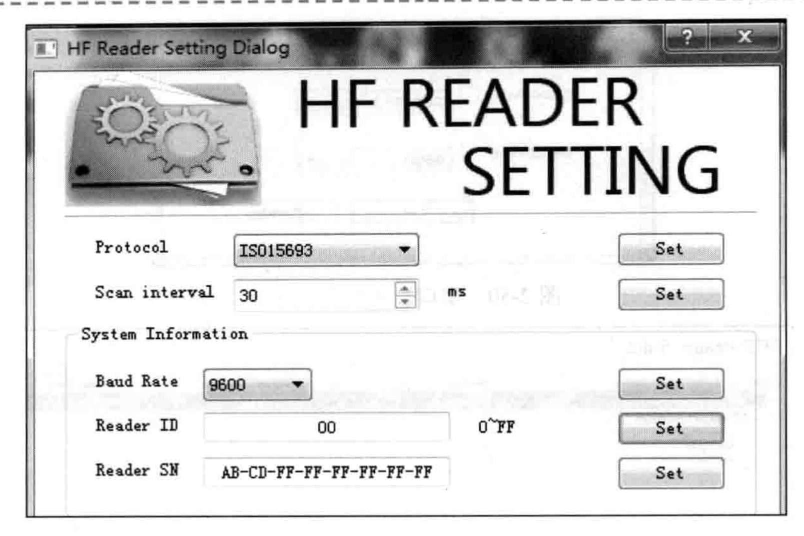


图 2-53　高频读写器设置界面

步骤 5：在图 2-54 中选择协议和设置读取间隔后，单击“Set”按钮确认设置。

Protocol　ISO15693　Set
Scan interval　30　ms　Set

图 2-54　协议和设置读取间隔界面

步骤 6：读取系统信息。系统信息的输入框中默认显示的是读取到的系统信息，如图 2-55 所示。

System Information
Baud Rate　9600　Set
Reader ID　00　0~FF　Set
Reader SN　FF-FF-FF-FF-FF-FF-FF-FF　Set

图 2-55　系统信息

步骤 7：设置读写器的波特率。有五种波特率可选，分别是 9600 波特、19200 波特、38400 波特、57600 波特和 115200 波特。选择 115200 波特，单击右侧“Set”按钮。

步骤 8：设置机器 ID 号，在对应的输入框中，以十六进制数据格式输入 1 字节，单击右侧对应的“Set”按钮。

步骤 9：设置机器序列号，在对应的输入框中，以十六进制数据格式输入 8 字节，单击右侧“Set”按钮。

步骤 10：记录步骤 5～步骤 8 的结果。



2.3.5 实训五：低频读写器的基本认知

1. 任务目标

了解低频读写器的基本原理，学会如何使用低频读写器。

2. 设备准备

（1）RFID 实验箱。
（2）计算机一台。
（3）低频标签一张。

3. 任务实施

步骤 1：启动读写器。打开 RFID 实验箱，连接好实验箱和计算机，启动电源。
步骤 2：打开读写器后台控制软件，选择低频模块，如图 2-56 所示。



图 2-56 读写器控制软件

步骤 3：选择低频模块对应的串口（弹出的显示值即对应串口），这里为 COM7，如图 2-57 所示。

步骤 4：将标签放置在低频读写器的天线上，单击 Start scan，移动标签位置，观察读取情况，如图 2-58 所示。

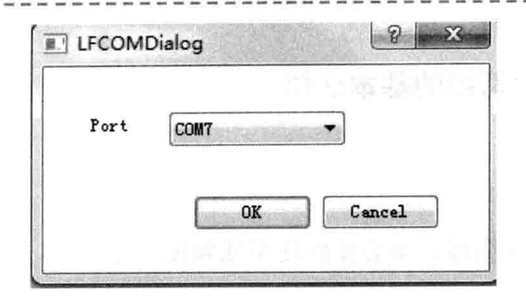


图 2-57　串口选择

Reader	Hardware	Software	Action	State
LF 00-00-00-00	LF hardware	LF firmware	Idle	Online
Reader Information				
Different Tags	1			
Read Count	6			
Reads per second	0			
02-41-00-0F-E1-B1-03				
Read Count	6			

图 2-58　读取标签

步骤 5：记录步骤 4 的结果。

2.4　练习题

1．图 2-59 为 RFID 系统结构图，请将电子标签、天线、读写器、数据填入图 2-59 中①～④项。

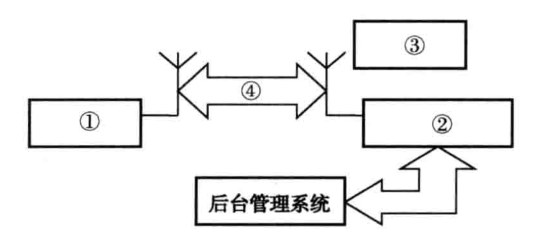


图 2-59　RFID 系统图

①______________________　②______________________

③______________________　④______________________。

2．比较 RFID 与常见的自动识别技术性能，并填写表 2-10。

表 2-10　自动识别技术性能比较

性能参数	条　形　码	生物识别	IC 卡	RFID
典型的数据量（Byte）				
读写性能				
污染和潮湿的影响				

续表

性能参数	条 形 码	生物识别	IC卡	RFID
遮盖的影响				
方向的影响				
位置的影响				
退化和磨损的影响				
购买成本				
运行成本				
安全性				
识别速度				
识别距离				
使用寿命				
识别数量（次）				

3．RFID的低频、高频、超高频和微波有各自标准和特性，请完成表2-11。

表2-11　RFID各波段标准和特性

内 容	低 频	高 频	超 高 频	微 波
工作频率				
市场占有率				
读取距离				
速度				
潮湿环境				
方向性				
全球适用频率（是，地区）				
现有ISO标准				
主要应用范围				

4．根据主动式标签的特点，请填写表2-12。

表2-12　主动式标签的特性

代 次	特 性
1st	
2nd	
3rd	
……	

5．选择某种RFID读写器，如SR–7114车载读写器，根据产品填充下列空白，以掌握RFID设备常见的参数。

物理环境指标：

■ 工作温度：

■ 存储温度：

■ 工作湿度：

■ 工作电源：

■ 尺寸/重量：

■ 外壳材料：金属（合金铝）。

主要性能指标：

■ 空中接口协议：

■ 频率特征：国标：（　　）MHz~（　　）MHz，信道间隔：（　　）kHz。

美标：（　　）MHz~（　　）MHz，信道间隔：（　　）kHz。

■ 频率模式：定频/跳频，（　　）个跳频点。

■ 输出功率：（　　）~（　　）dBm，步进间隔（　　）dB。

■ 读写标签距离：读标签距离>（　　）米（与天线和标签有关），写标签约为读标签距离的（　　）%。

■ 天线端口：（　　）个 SMA 接口。

■ 通信接口：（　　）个。

■ 工作模式：外部触发/间隔 T 循环/连续工作。

■ 输入/输出口：（　　）光电隔离输入。

6．将下段有关 RFID 中文翻译成英文。

RFID（射频识别）是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，识别工作无须人工干预，作为条形码的无线版本，RFID 技术具有条形码所不具备的防水、耐高温、使用寿命长、读取距离大、标签上数据可以加密、存储数据容量更大、存储信息更改自如等优点，其应用将给零售、物流等产业带来革命性变化。

译文：____

____

____

____

____。

7．在完成实训三的基础上，回答下面两个问题。

（1）修改标签 EPC 的操作有什么用途？如果有多只，你将如何修改这些标签的 EPC 使之简单易懂？

答：____

____。

（2）标签的 EPC 共有多少位？利用该区域最多可以对多少物品进行标识？

答：____

____

____。



8．探究读写器频率对标签读取距离的影响。读写器天线和标签天线均存在最佳响应频段，在最佳响应频段内可以获得较好的读取距离。当工作频率偏离天线设计的工作频率范围时，会引起天线参数的变化，例如引起方向图的变形、输入阻抗的改变等，从而引起辐射范围的改变。改变 RFID 读写器的工作频率，此时 RFID 读写器对 RFID 标签读取的距离会受影响。

（1）系统设置。打开读写器后台控制软件，RFID 读写器后台控制软件和 RFID 读写器连接成功后，选中标签，将读写器的起始频率设置为 840.125kHz，结束频率设置为 844.875kHz，如图 2-60 所示。

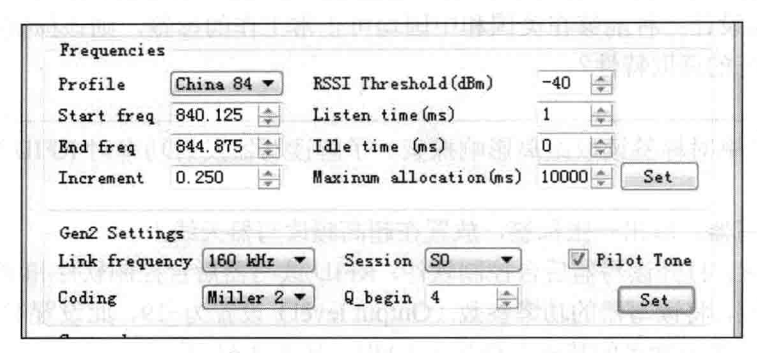


图 2-60　读写器频率设置

（2）测量距离。改变 RFID 标签平面与 RFID 读写器平面之间的垂直距离，直到 RFID 读写器刚好能够读到 RFID 标签，测量 RFID 读写器天线与 RFID 标签之间的距离（单位为厘米），将该数据记录到表 2-13 中。

（3）更改频率。依次将频率更改为 890.750kHz～900.250kHz，900.750kHz～910.250kHz，910.750kHz～927.250kHz，927.250kHz～940.250kHz。将所测得的数据记录到表 2-13 中。

（4）更改标签。依次替换不同型号的标签，放置在读写器前，重复步骤（1）～步骤（3）。并将所测得的数据记录到表 2-13 中。

表 2-13　RFID 读写器频率的改变对 RFID 标签读取距离的影响记录表

序　　号	标签型号	890.750kHz～900.250kHz（读取距离厘米）	900.750kHz～910.250kHz（读取距离厘米）	910.750kHz～927.250kHz（读取距离厘米）	927.750kHz～940.250kHz（读取距离厘米）
1					
2					
3					
4					
5					

（5）对照图 2-60，回答下列问题：

① 单击“Profile”下拉式按钮，查出各国为超高频 RFID 划分的工作频段是如何规定的，哪个国家为超高频 RFID 划分的频段最宽？

答：____

____。

② 实验箱使用的天线的设计适用工作频段为多少？

答：____。

③ 某厂商拟设计一种能够在美国和中国均可正常工作的标签，则该标签应当设计至少在哪个频段具有较好的读取特性？

答：____。

9. 读写器功率对标签读取距离影响探索。了解读写器发射功率对 RFID 标签读取距离的影响。

（1）启动读写器，取出一张标签，放置在超高频读写器天线上。

（2）系统设置。打开读写器后台控制软件，RFID 读写器后台控制软件和 RFID 读写器连接成功后，选中标签，将读写器的功率参数（Output level）设置为-19，此设置对应的含义为读写器输出功率在最大输出功率的基础上衰减了 19dB，如图 2-61 所示。

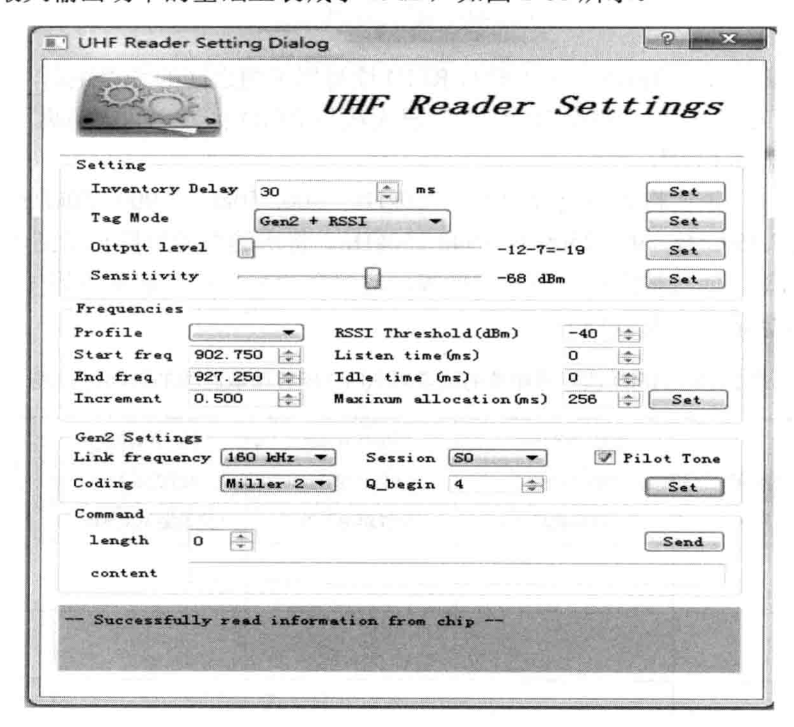


图 2-61　UHF 读写器设置

（3）测量距离。移动标签远离天线，改变 RFID 标签平面与 RFID 读写器天线之间的垂直距离，直到 RFID 读写器刚好能够读到 RFID 标签，此时标签到读写器天线之间的距离即最大读取距离；测量最大读取距离（单位为厘米），将该数据记录到表 2-14 中。

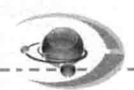


表 2-14　RFID 读写器功率的改变对 RFID 标签读取距离的影响记录表

序　号	标签型号	−19 （读取距离 cm）	−15 （读取距离 cm）	−10 （读取距离 cm）	−5 （读取距离 cm）	0 （读取距离 cm）
1						
2						
3						
4						
5						

（4）更改功率。依次将 Output level 更改为-15，-10，-5，0，重复步骤（3），并将所有测得的距离记录到表 2-14 中。

（5）更改标签。依次将不同型号的标签放在读写器前，重复步骤（3）～步骤（4），并将所有测得的数据记录到表 2-14 中。

（6）根据上述结果，思考下面两个问题。

① Output level 设置为 0 时读写器端口对应的输出功率约为 30dBm（即 1000mW），假设 Output level 设置为−30 时对应的输出功率应该为多少？

答：____

____。

② 从理论上进行计算，Output level 设置为−3 时，对应的输出功率是设置为 0 时输出功率的 1/2 吗？为什么？

答：____

____。

第3章

物联网传感器技术

最早的传感器出现在 1861 年，作为连接物理世界与电子世界的重要媒介，在当今信息化的过程中发挥着关键作用。事实上，传感器已经渗透到人们当今的日常生活中。只要细心观察，就可以发现日常生活中的各类传感器，例如热水器的温控器、电视机的遥控器、空调的温湿度传感器等。此外，传感器也广泛应用到工农业、医疗卫生、军事国防、环境保护等领域，极大地提高了人类认识世界和改造世界的能力。

现代信息技术智能化表现在以下几个方面。

（1）感测技术：获取信息的技术（感官）。

（2）通信技术：传递信息的技术（神经）。

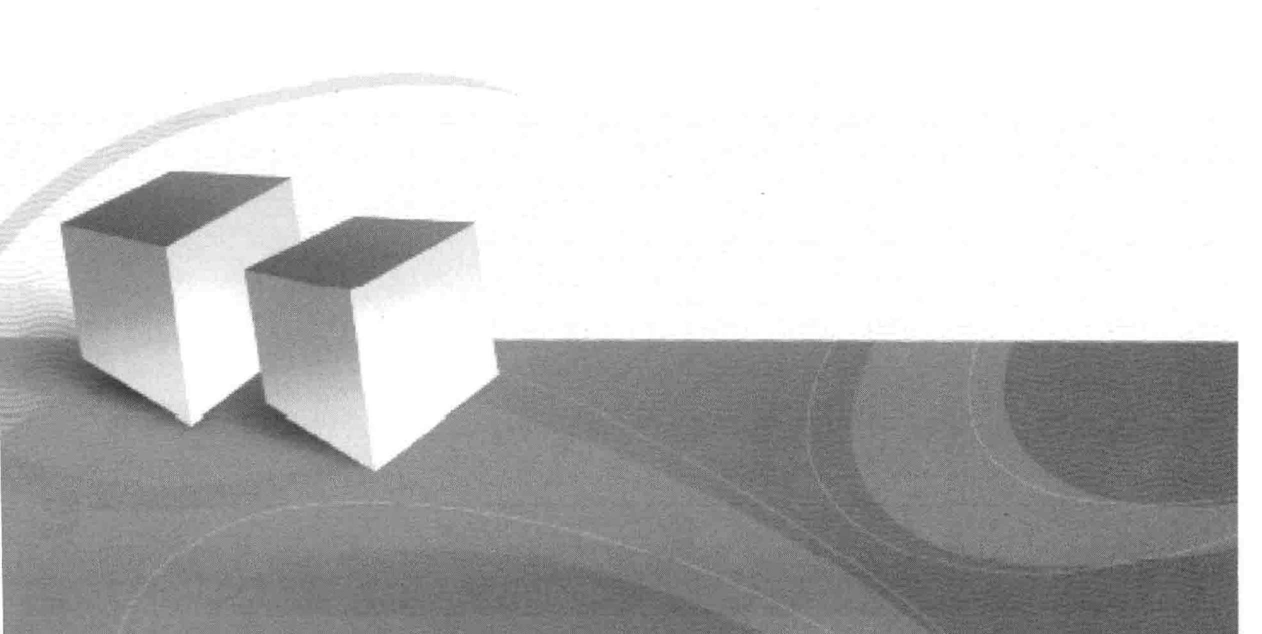
（3）计算机技术：处理信息的技术（大脑）。

（4）控制技术：利用信息的技术（大脑的决策）。

计算机技术＋传感器技术→智能传感器

计算机技术＋通信技术→计算机网络技术

计算机网络技术＋智能传感器→网络化智能传感器





3.1　传感器技术

3.1.1　什么是传感器

国际电工委员会（International Electro-technical Committee，IEC）认为："传感器是测量系统中的一种前置部件，它将输入变量转换成可供测量的信号"。按照 Gopel 等的说法："传感器是包括承载体和电路连接的敏感元件"，而"传感器系统则是组合有某种信息处理（模拟或数字）能力的传感器"。传感器是传感器系统的最重要组成部分，它是被测量信号输入的第一道关口。

国家标准（GB 7665-2005）对"传感器"的定义：能感受规定的被测量并按照一定的规律转换成可用输出信号的器件或装置。

传感器是检测系统的第一环节。它是以一定的精度把被测量转换成与之有确定关系的、便于应用的某种量值的测量装置。顾名思义，传感器的功能是"一感二传"，即感受被测信息，并传送出去。根据传感器的功能要求，它一般应由三部分组成，即敏感元件、转换元件和转换电路，如图 3-1 所示。

（1）敏感元件。它是直接感受被测量，并输出与被测量成确定关系的某一物理量的元件。

（2）转换元件。敏感元件的输出就是它的输入，它把输入转换成电路参量。

（3）转换电路。电路参数接入基本转换电路（简称转换电路），便可转换成电量输出。传感器只完成被测参数至电量的基本转换，然后输入到测控电路，进行放大、运算、处理等进一步转换，以获得被测值或进行过程控制。

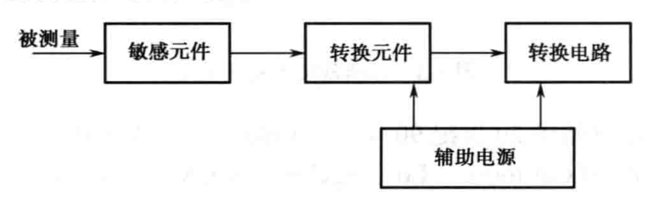


图 3-1　传统传感器组成

传感器作为信息获取的重要手段，与通信技术和计算机技术共同构成了信息技术的三大支柱。然而，传统传感器网络化、智能化的程度十分有限。具体来说，传统传感器网络化、智能化的程度十分有限，缺少有效的数据处理与信息共享能力。现代传感器伴随着微电子机械系统（Micro Electro Mechanical Systems，MEMS）、超大规模集成电路（Very Large Scale Integrated Circuits，VLSI）的发展，使得现代传感器走上微型化、智能化和网络化的发展路线，其典型的代表是无线传感器节点（Wireless Sensor Nodes）。

和传统的传感器不同，无线传感器节点不仅包括了传感器部件，而且集成了微型处理器和无线通信芯片等，能够对感知的信息进行分析处理和网络传输，如图 3-2 所示。

网络化催生了全新的传感器应用模式——传感网。无线传感网是由部署在监测区域内的大

量微型、低成本、低功率的传感器节点组成的多跳无线网络。它主要用于长期、实时、大规模、自动化的环境监测。

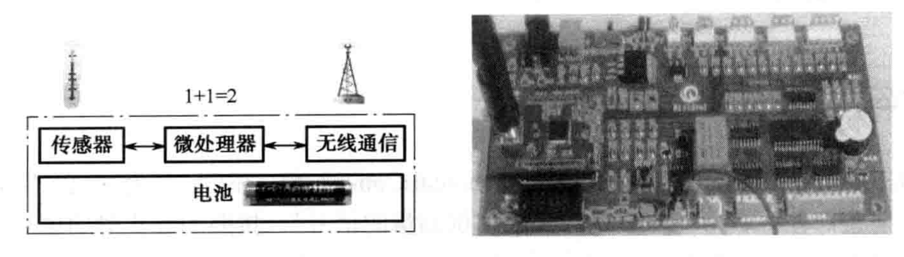


图 3-2　无线传感器节点组成

3.1.2　传感器简史

传感器技术发展沿着图 3-3 中两条主线展开。

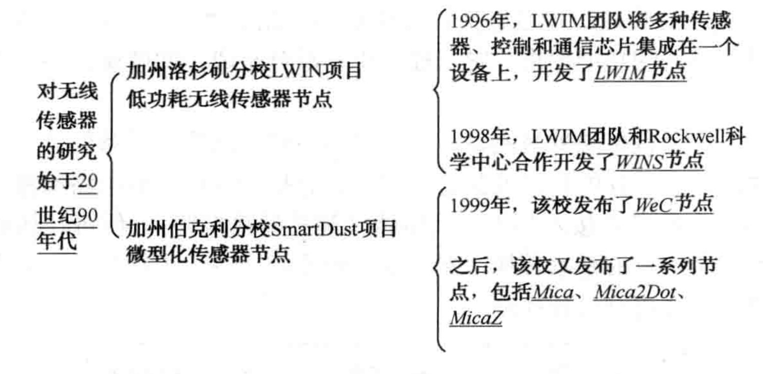
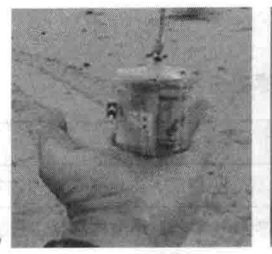


图 3-3　传感器技术发展主线

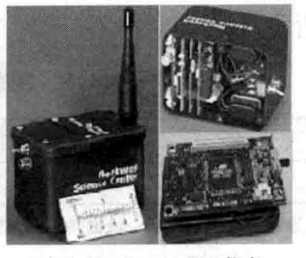
对无线传感器的研究始于 20 世纪 90 年代。1996 年，在美国国防部的资助下，加州大学洛杉矶分校（University of California，Los Angeles，UCLA）开展了旨在开发低功耗的无线传感器设备的 LWIM（Low-power Wireless Integrated Microsensors）项目。LWIM 团队将多种传感器、控制和通信芯片集成在一个设备上，开发了 LWIM 节点。两年后，LWIM 团队和 Rockwell 科学中心合作开发了 WINS（Wireless Integrated Network Sensors）节点（见图 3-4）。该节点使用 Intel StrongARM 32 位的处理器（1MB 的内存和 4MB 的内存），100Kb/s 数据率的通信芯片，具有较强的信息处理能力。在正常和睡眠状态下，处理器的功率分别为 200mW 和 0.8mW。

同时，加州大学伯克利分校（UCB）发起了“智慧尘埃”（Smart Dust）项目，旨在开发微型化的传感器节点。1999 年，该校发布了 WeC 节点。该节点使用 8 位 Atmel 系列的微型处理器（512KB 的内存和 8KB 的闪存）。在正常和睡眠状态下，处理器的功率分别仅为 15mW 和 45uW。之后，该校又发布了一系列微型化、低功率的节点平台，包括后来被研究者广泛使用的 Mica、Mica2Dot 和 MicaZ。





（a）LWIM Ⅲ节点



（b）Rockwell WINS节点

图 3-4　UCLA 制作的节点

摩尔先生于 1965 年 4 月 19 日预测，半导体芯片上集成的晶体管和电阻数量将每年翻一番。1975 年又提出修正，芯片上集成的晶体管数量将每两年翻一番（实为 18 个月），这就是摩尔定律。40 年来，计算机从神秘不可近的庞然大物变成多数人都不可或缺的工具，充分论证了摩尔定律。然而，从传感器节点的发展历史看，节点的性能并没有按照摩尔定律预测的速度发展。1999 年，WeC 节点采用 8 位 4MHz 主频的处理器，2002 年 Mica 节点采用 8 位 7.37MHz 的处理器，2004 年 Telos 节点采用 16 位 4MHz 的处理器。Telos 节点仍然是目前普遍采用的传感器节点。传感器节点的发展曲线如图 3-5 所示。从图中不难看出，节点性能的提升十分缓慢。原因何在？事实上，传感器节点性能的提升主要受到表 3-1 中因素制约。

表 3-1　无线传感器节点制约因素

制约因素	原因说明
功耗	无线传感器节点一般部署于野外，不能通过有线供电。硬件设计须以节能为重要设计目标。如，在正常工作模式下，WeC、Mica 和 Telos 节点处理器功率仅为 15mW、8mW 和 3mW
价格	无线传感节点一般需要大量组网以完成特定的功能，其硬件设计必须以廉价为重要设计目标。价格的因素制约了传感器节点的功能
体积	无线传感节点一般需要容易携带，易于部署。其硬件设计必须以微型化为重要设计目标。体积的因素制约了传感器节点的功能

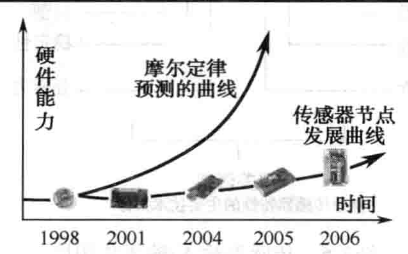


图 3-5　传感器节点的发展曲线

3.1.3　传感器分类

可以用不同的观点对传感器进行分类：工作原理、用途、输出信号类型以及制作它们的材

料和工艺等，如表 3-2 所示。

表 3-2　传感器分类

类　型	种　类
工作原理	应变式、电容式、电感式、热电式、光电式、压电式、磁电式、超声波等
用途	力敏传感器、位置传感器、液面传感器、能耗传感器、速度传感器、热敏传感器、振动传感器、加速度传感器、射线辐射传感器、真空度传感器、生物传感器等
输出信号	模拟传感器、数字传感器、膺数字传感器、开关传感器等
制造工艺	集成传感器、薄膜传感器、厚膜传感器、陶瓷传感器等

3.1.4　传感器特性

1. 传感器静态特性

传感器的静态特性是指对静态的输入信号，传感器的输出量与输入量之间具有的相互关系。因为这时输入量和输出量都和时间无关，所以它们之间的关系，即传感器的静态特性可用一个不含时间变量的变换关系表示，如图 3-6 所示。

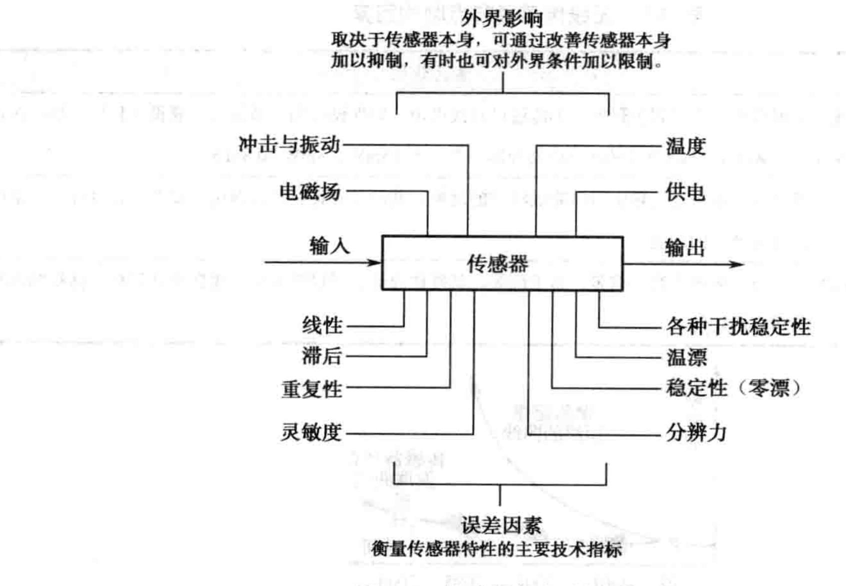


图 3-6　传感器输入/输出作用图

人们总希望传感器的输入与输出呈唯一的对应关系，而且最好呈线性关系。但一般情况下，输入/输出不完全符合所要求的线性关系。因为传感器本身存在着迟滞、蠕变、摩擦等各种因素，以及受外界条件的各种影响。因此表征传感器静态特性的主要参数有：线性度、灵敏度、迟滞性、重复性、漂移性等，如表 3-3 所示。



表 3-3 传感器静态特性

特 性	内 容	图 示
线性度	指传感器输出量与输入量之间的实际关系曲线偏离拟合直线的程度。定义为在全量程范围内实际特性曲线与拟合直线之间的最大偏差值与满量程输出值之比	
灵敏度	灵敏度是传感器静态特性的一个重要指标。其定义为输出量的增量与引起该增量的相应输入量增量之比	
迟滞性	传感器在输入量由小到大（正行程）及输入量由大到小（反行程）变化期间其输入输出特性曲线不重合的现象称为迟滞。对于同一大小的输入信号，传感器的正反行程输出信号大小不相等，这个差值称为迟滞差值	
重复性	重复性是指传感器在输入量按同一方向作全量程连续多次变化时，所得特性曲线不一致的程度	
漂移性	传感器的漂移是指在输入量不变的情况下，传感器输出量随着时间变化，此现象称为漂移。产生漂移的原因有两个：一是传感器自身结构参数（如称重器的弹性退化）；二是周围环境（如我国南北方温度、湿度的差异等）	

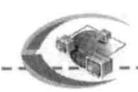
2. 传感器动态特性

传感器动态特性是指传感器对随时间变化的输入量的响应特性。在实际工作中，传感器的动态特性常用它对某些标准输入信号的响应来表示。这是因为传感器对标准输入信号的响应容易用实验方法求得，并且它对标准输入信号的响应与它对任意输入信号的响应之间存在一定的关系，往往知道了前者就能推定后者。最常用的标准输入信号有阶跃信号和正弦信号两种，所以传感器的动态特性也常用阶跃响应和频率响应来表示。

3.1.5 选用原则

1. 根据测量对象与测量环境确定传感器的类型

要进行具体的测量，需要根据被测量的特点和传感器的使用条件考虑以下一些具体问题：量程的大小；被测位置对传感器体积的要求；测量方式为接触式还是非接触式；信号的引出方法，有线或是非接触测量；传感器的来源，国产还是进口，价格能否承受。在考虑这些问题之后就能确定选用何种类型的传感器，然后再考虑传感器的具体性能指标。



2. 灵敏度的选择

通常，在传感器的线性范围内，希望传感器的灵敏度越高越好。因为只有灵敏度高时，与被测量变化对应的输出信号的值才比较大，有利于信号处理。但要注意的是，传感器的灵敏度高，与被测量无关的外界噪声也容易混入，也会被放大系统放大，影响测量精度。因此，要求传感器本身应具有较高的信噪比，尽量减少从外界引入的干扰信号。

3. 频率响应特性

传感器的频率响应特性决定了被测量的频率范围，必须在允许频率范围内保持不失真的测量条件，实际上传感器的响应总有一定延迟，希望延迟时间越短越好。

传感器的频率响应高，可测的信号频率范围就宽，而由于受到结构特性的影响，机械系统的惯性较大，因此固有频率低的传感器可测信号的频率较低。

4. 线性范围

传感器的线性范围是指输出与输入成正比的范围。但任何传感器都不能保证绝对的线性，其线性度也是相对的。当所要求测量精度比较低时，在一定的范围内，可将非线性误差较小的传感器近似看做线性的，这会给测量带来极大的方便。

5. 稳定性

传感器使用一段时间后，其性能保持不变化的能力称为稳定性。影响传感器长期稳定性的因素除传感器本身结构外，主要是传感器的使用环境。因此，要使传感器具有良好的稳定性，传感器必须要有较强的环境适应能力。

6. 精度

精度是传感器的一个重要的性能指标，它是关系到整个测量系统测量精度的一个重要环节。传感器的精度越高，其价格越昂贵，因此，传感器的精度只要满足整个测量系统的精度要求就可以，不必选得过高。这样就可以在满足同一测量目的的诸多传感器中选择比较便宜和简单的传感器。

3.1.6 大规模长时间部署传感器的设计需求

1. 低成本与微型化

- 低成本的节点才能被大规模部署，微型化的节点才能使部署更加容易。
- 节点的软件设计也需要满足微型化的需求。例如 TelosB 节点的内存大小只有 4KB，程序存储的空间只有 10KB。因此，节点程序的设计必须节约计算资源，避免超出节点的硬件能力。



2. 低功耗

- 在硬件设计上采用低功耗芯片。例如 TelosB 节点使用的微处理器，在正常工作状态下功率为 3mW，而一般的计算机的功率为 200W～300W。
- 通过软件节能策略来实现节能。软件节能策略的核心就是尽量使节点在不需要工作的时候进入低功耗模式，仅在需要工作的时候进入正常状态。

3. 灵活性与扩展性

- 传感器节点被用于各种不同的应用中，因此节点硬件和软件的设计必须具有灵活性和扩展性。
- 节点的硬件设计须满足一定的标准接口，例如节点和传感板的接口统一有利于给节点安装上不同功能的传感器。
- 软件的设计必须是可剪裁的，能够根据不同应用的需求，安装不同功能的软件模块。

4. 稳定性

- 稳定性是实现传感器网络长时间部署的重要保障。
- 对于普通的计算机，一旦系统崩溃了，人们可以采用重启的方法恢复系统，而传感器节点则不行，就整个网络而言，可以适当增加冗余性，增加整体系统的稳定性和安全性。

3.2 ZigBee 协议

3.2.1 ZigBee 基础知识

1. ZigBee 信道

IEEE 802.15.4 定义了两个物理层标准，分别是 2.4GHz 物理层和 868/915MHz 物理层。两者均基于直接序列扩频（Direct Sequence Spread Spectrum，DSSS）技术。

ZigBee 使用了 3 个频段，定义了 27 个物理信道，其中 868MHz 频段定义了一个信道；915MHz 频段附近定义了 10 个信道，信道间隔为 2MHz；2.4GHz 频段定义了 16 个信道，信道间隔为 5MHz。具体信道分配如表 3-4 所示。

表 3-4 ZigBee 信道分配

信道编号	中心频率/MHz	信道间隔/MHz	频率上限/MHz	频率下限/MHz
k=0	868.3		868.6	868.0
k=1,2,3…10	906+2（k−1）	2	928.0	902.0
k=11,12,13…26	2401+5（k−11）	5	2483.5	2400.0

其中，2.4GHz的物理层数据传输速率为250Kb/s。915MHz的物理层数据传输速率为40Kb/s。868MHz 的物理层数据传输速率为 20Kb/s。

2. ZigBee PANID

PANID（Personal Area Network ID）是网络的 ID（即网络标识符）。针对一个或多个应用网络，它用于区分不同的 ZigBee 网络。所有节点的 PANID 唯一，一个网络只有一个 PANID，它是由协调器生成的。PANID 是可选配置项，用来控制 ZigBee 路由器和终端节点要加入哪个网络。

PANID 是一个 32 位标识，范围为 0x0000～0xFFFF。

3. ZigBee MAC 地址

ZigBee 设备有两种类型的地址：物理地址和网络地址。

物理地址是一个 64 位 IEEE 地址，即 MAC 地址，通常称为长地址。64 位地址是全球唯一的地址，设备将在它的生命周期中一直拥有它。它通常由制造商或者被安装时设置。这些地址由 IEEE 来维护和分配。

16 位网络地址是当设备加入网络后分配的，通常称为短地址。它在网络中是唯一的，用来在网络中鉴别设备和发送数据，当然，不同的网络 16 位短地址可能相同。

4. ZigBee 设备类型

ZigBee 设备类型有三种：协调器、路由器和终端节点。

（1）ZigBee 协调器（Coordinator）。

协调器是整个网络的核心，是 ZigBee 网络的第一个开始的设备。它选择一个信道和网络标识符（PANID），建立网络，并且对加入的节点进行管理和访问，对整个无线网络进行维护。在同一个 ZigBee 网络中，只允许一个协调器工作，当然它也是不可缺的设备。图 3-7 所示为 ZigBee 协调器。

（2）ZigBee 路由器（Router）。

ZigBee 路由器的作用是提供路由信息（见图 3-8）。

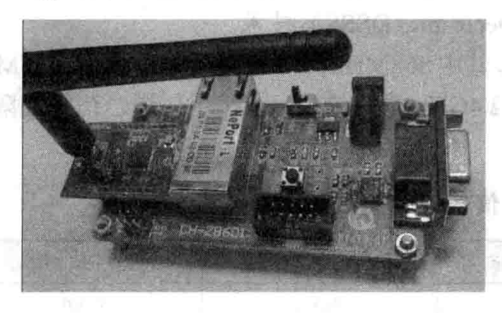


图 3-7　ZigBee 协调器

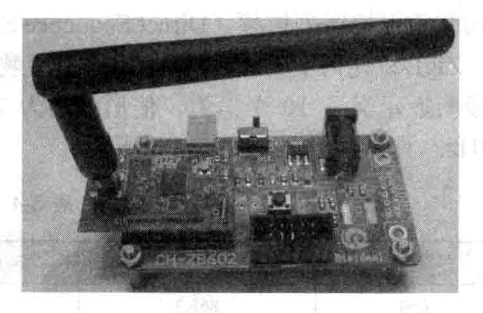


图 3-8　ZigBee 路由器

（3）ZigBee 终端节点（End-Device）。

图 3-9 所示的 ZigBee 终端节点没有路由功能，完成的是整个网络的终端任务。



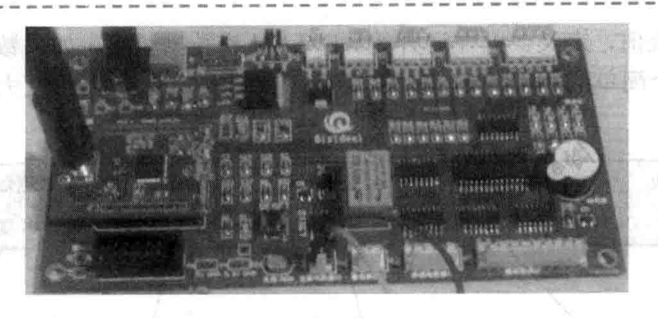


图 3-9　ZigBee 终端节点

5. ZigBee 网络的形成

首先，由 ZigBee 协调器建立一个新的 ZigBee 网络。一开始，ZigBee 协调器会在允许的通道内搜索其他的 ZigBee 协调器。并基于每个允许通道中所检测到的通道能量及网络号，选择唯一的 16 位 PANID，建立自己的网络。新网络一旦被建立，ZigBee 路由器与终端设备就可以加入到网络中了。

网络形成后，可能会出现网络重叠及 PANID 冲突的现象。协调器可以初始化 PANID 冲突解决程序，改变一个协调器的 PANID 与信道，同时相应修改其所有的子设备。

通常，ZigBee 设备会将网络中其他节点信息存储在一个非易失性的存储空间——邻居表中。加电后，若子节点曾加入过网络，则该设备会执行孤儿通知程序来锁定先前加入的网络。接收到孤儿通知的设备检查它的邻居表，并确定设备是不是它的子节点，若是，设备会通知子节点其在网络中的位置，否则子节点将作为一个新设备来加入网络。而后，子节点将产生一个潜在双亲表，并尽量以合适的深度加入到现存的网络中。

设备检测通道能量所花费的时间与每个通道可利用的网络可通过 ScanDuration 扫描持续参数来确定，一般设备要花费 1 分钟的时间来执行一个扫描请求，对于 ZigBee 路由器与终端设备来说，只需要执行一次扫描即可确定加入的网络。而协调器则需要扫描两次，一次采样通道能量，另一次则用于确定存在的网络。

3.2.2　PC 端数据访问接口协议

串口通信设置。

- 波特率：38400。
- 校验位：无校验。
- 数据位：8 位。
- 停止位：1 位。

1. PC 端接收数据格式

PC 端接收数据格式如下：

SOP	D_LEN	DATA	CHECK

SOP 为操作系统值，定义数据发送开始。D_LEN 为数据长度，如果数据长度小于 7，则表示该帧数据只是一个简单的 ACK 帧。DATA 表示纯数据。如果数据长度大于 7，则 DATA 段表示如下：

标志	长度	串口接收对象	网络地址		数据对象	命令标识		数据负荷长度	数据负荷	校验位
			低位	高位		低位	高位			

ENDP	LO_ADDR	HI_ADDR	EP	LO_ID	HI_ID	LEN	DAT

其中，

ENDP：终端节点标号。

LO_ADDR-HI_ADDR：短地址。

EP：终端节点标号。

LO_ID-HI_ID：簇 ID 标号。具体定义如下：

✧ LOCATION_END-DEVICE_DEFAULT	0x0020	预留簇 ID
✧ LOCATION_END-DEVICE_TEMPRATURE	0x0030	温度 ID
✧ LOCATION_END-DEVICE_HUMIDITY	0x0031	温湿度 ID
✧ LOCATION_END-DEVICE_LUMINOSITY	0x0032	板载光照度 ID
✧ LOCATION_END-DEVICE_PIRSENSOR	0x0033	红外人体感应 ID
✧ LOCATION_END-DEVICE_GASSENSOR	0x0034	气体传感器 ID
✧ LOCATION_END-DEVICE_GHGBUTTON		干簧管按键 ID
✧ LOCATION_END-DEVICE_HUMTEMP	0x0036	温湿度 ID
✧ LOCATION_END-DEVICE_LED	0x0041	LED 控制 ID
✧ LOCATION_END-DEVICE_BUZZER	0x0042	蜂鸣器控制 ID
✧ LOCATION_END-DEVICE_DCMOTOR	0x0043	直流电机控制 ID
✧ LOCATION_END-DEVICE_STEPMOTOR	0x0046	步进电机控制 ID
✧ LOCATION_END-DEVICE_ADDRMAP	0x0050	长短地址匹配 ID
✧ LOCATION_COORDINATOR_PANID	0x0051	获取 PANIDID
✧ LOCATION_COORDINATOR_NODENUM	0x0052	获取节点数 ID
✧ LOCATION_COORDINATOR_CHANNEL	0x0053	获取信道 ID
✧ LOCATION_COORDINATOR_LOCADDR	0x0054	获取协调器 MAC 地址 ID

LEN：数据负荷长度。

DAT：数据负荷。

CHECK：校验和。校验和计算方法：去除操作系统值 SOP，然后进行异或计算。

2. PC 端发送数据格式

PC 端发送数据格式类同于接收数据格式，表示如下：

SOP	D_LEN	DATA	CHECK



SOP：0x02 为操作系统值，定义数据发送开始。D_LEN 代表数据长度，如果数据长度小于 7，则表示该帧数据只是一个简单的 ACK 帧。DATA 表示纯数据。如果数据长度大于 7，则 DATA 段表示如下：

ENDP	LO_ADDR	HI_ADDR	EP	LO_ID	HI_ID	LEN	DAT

其中，

ENDP：终端节点标号，指定为 0xCB。

LO_ADDR-HI_ADDR：短地址。

EP：终端节点标号，0xD2——路由节点，0xD3——传感控制节点，0xCB——协调器。

LO_ID-HI_ID：簇 ID 标号，同数据发送格式。

LEN：数据负荷长度。

DAT：数据负荷。

CHECK：校验和。校验和计算方法：去除操作系统值 SOP，然后进行异或计算。

3.3 实训

3.3.1 实训一：组建星型 ZigBee 网络

1. 任务目标

（1）了解 ZigBee 星型网络通信原理及相关技术。利用 1 个 ZigBee 协调器、多个传感控制节点组建一个简单的星型网络，并观察射频顶板上 LED 指示灯的变化。

（2）了解 ZigBee 星型网络组建的基本过程和方法。利用上位机软件，查看生成的网络拓扑。

2. 设备准备

（1）ZigBee 套件：协调器、传感控制节点。

（2）操作台：提供电源、PC、USB 口，以及多种传感器和输入/输出控制器件。

（3）软件：上位机软件。

3. 网络拓扑结构

网络拓扑结构如图 3-10 所示。

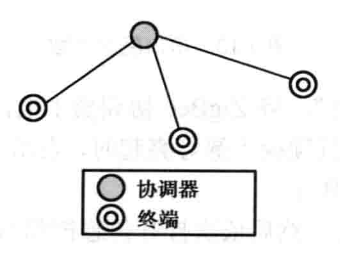


图 3-10　星型网络拓扑结构

4. **任务实施**

步骤 1：首先，将 ZigBee 协调器通过串口 RS232 与上位机连接。其次，运行上位机软件“ZigBee 基础实验平台软件”，在“选择串口”后的下拉列表中选择相应的串口（与实验台上的串口标号保持一致），并打开串口，如图 3-11 所示。打开操作台上 ZigBee 协调器，然后依次打开传感控制节点，加入协调器所建立的 ZigBee 网络，生成如图 3-10 所示的简单星型网络拓扑结构。

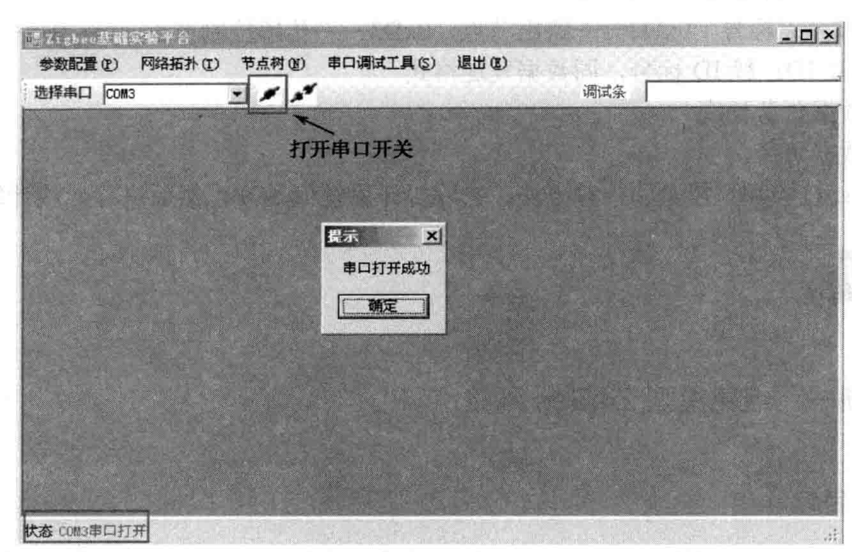


图 3-11　打开串口

步骤 2：单击菜单栏中“参数配置”，查看参数配置，串口参数设置如图 3-12 所示。

图 3-12　串口配置参数

步骤 3：打开“串口调试工具”，将 ZigBee 协调器上电，当射频顶板上红灯亮起时，依次打开 ZigBee 终端节点，当节点射频顶板上绿灯亮起时，表示节点已成功加入网络。此时查看工具窗口中的返回数据，如图 3-13 所示。

步骤 4：打开 ZigBee 协调器，然后依次打开传感控制节点，加入协调器所建立的 ZigBee 网络，生成简单的星型网络拓扑结构，如图 3-14 所示。



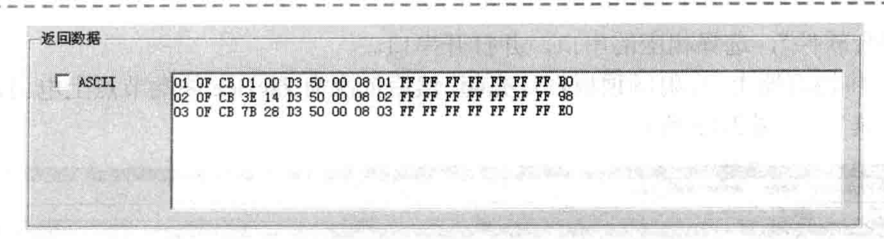


图 3-13　返回数据

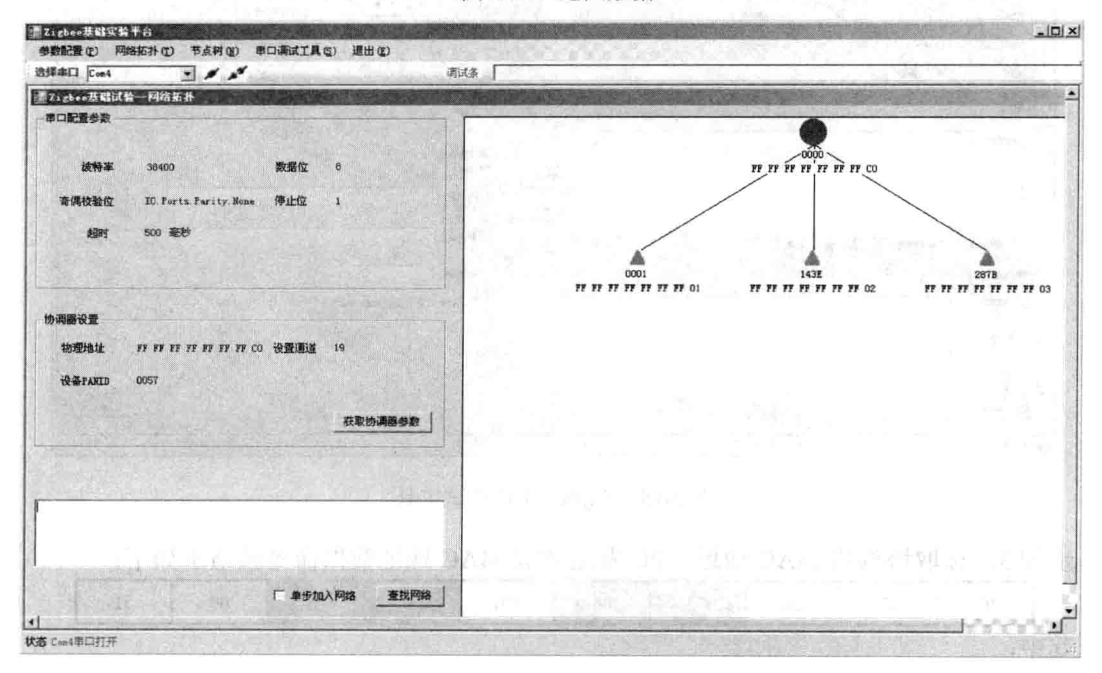


图 3-14　ZigBee 网络节点图与网络拓扑

3.3.2　实训二：ZigBee 模块基础信息读取

1. 任务目标

了解 ZigBee 节点设备类型、信道（Channel ID）、PANID、物理地址和网络地址。

2. 设备准备

（1）ZigBee 套件：协调器、传感控制节点。
（2）操作台：提供电源、PC、USB 口。
（3）软件：上位机软件。

3. 任务实施

步骤 1：首先将 ZigBee 协调器通过串口 RS232 与上位机连接。其次，运行上位机软件“ZigBee

基础实验平台软件”，选择相应的串口，并打开串口。

步骤 2：将协调器上电，射频顶板红灯亮起，然后依次为 ZigBee 终端节点上电。打开“ZigBee 串口调试工具”，如图 3-15 所示。

图 3-15　ZigBee 串口调试工具

步骤 3：读取协调器 MAC 地址。PC 发送获取 MAC 地址数据命令帧请求如下：

02	07	CB	00	00	CB	54	00	00	51

其中，

短地址 ADDR：0x0000；//0x0000 表示协调器。

终端节点号：0xCB，表示协调器。

ID：0x0051，表示获取协调器 MAC 地址。

数据负荷长度为 0。

在“发送指令”框的“示例指令”中，选择“获取 CB MAC 地址”，发送指令 02 07 CB 00 00 CB 54 00 00 51，如图 3-16 所示。

PC 接收地址返回如下：

00	0F	CB	00	00	CB	54	00	08	C0	FF	FF	FF	FF	FF	FF	FF	6C

其中，

数据负荷长度为 8。

协调器物理地址，即长地址为 FF FF FF FF FF FF C0。

步骤 4：读取信道。PC 发送信道命令帧请求为：

02	07	CB	00	00	CB	53	00	00	56

其中，

短地址 ADDR：0x0000。



终端节点号：0xCB，表示协调器节点。

ID：0x0053，表示读取信道。

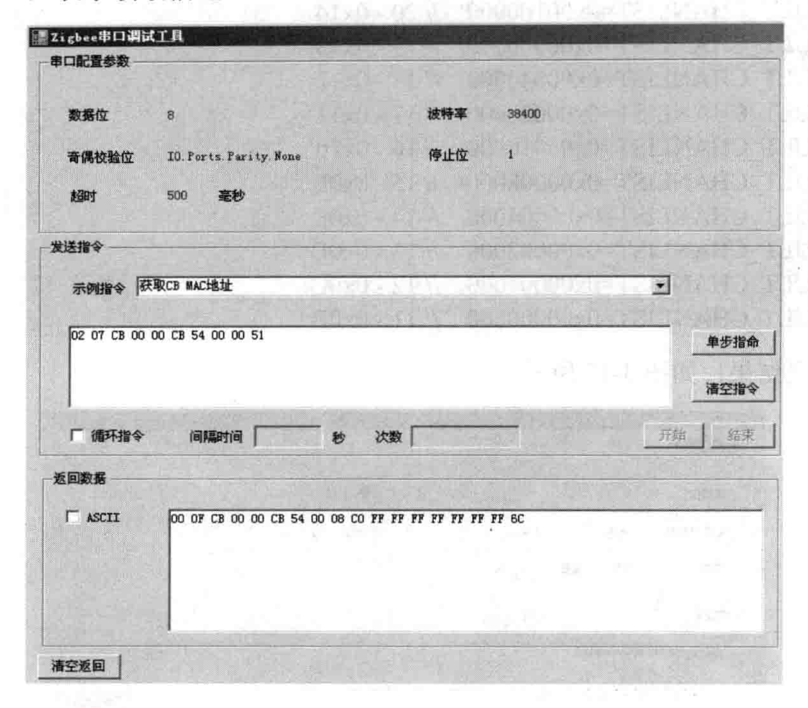


图 3-16　获取 CB MAC 地址

没有数据负荷。

PC 接收数据为：

01	09	CB	00	00	CB	53	00	04	00	00	00	02	5C

其中，

数据长度：0x04。

数据：0x02000000，与信道对应关系如下：

```
/* Default channel is Channel 11 - 0x0B */
// Channels are defined in the following:
//          0        : 868 MHz         0x00000001
//          1 - 10 : 915 MHz         0x000007FE
//        11 - 26 : 2.4 GHz          0x07FFF800
//
//-DMAX_CHANNELS_868MHZ          0x00000001
//-DMAX_CHANNELS_915MHZ          0x000007FE
//-DMAX_CHANNELS_24GHZ            0x07FFF800
-DDEFAULT_CHANLIST=0x04000000      // 26 - 0x1A
//-DDEFAULT_CHANLIST=0x02000000    // 25 - 0x19
//-DDEFAULT_CHANLIST=0x01000000    // 24 - 0x18
//-DDEFAULT_CHANLIST=0x00800000    // 23 - 0x17
```

```
//-DDEFAULT_CHANLIST=0x00400000   // 22 - 0x16
//-DDEFAULT_CHANLIST=0x00200000   // 21 - 0x15
//-DDEFAULT_CHANLIST=0x00100000   // 20 - 0x14
//-DDEFAULT_CHANLIST=0x00080000   // 19 - 0x13
//-DDEFAULT_CHANLIST=0x00040000   // 18 - 0x12
//-DDEFAULT_CHANLIST=0x00020000   // 17 - 0x11
//-DDEFAULT_CHANLIST=0x00010000   // 16 - 0x10
//-DDEFAULT_CHANLIST=0x00008000   // 15 - 0x0F
//-DDEFAULT_CHANLIST=0x00004000   // 14 - 0x0E
//-DDEFAULT_CHANLIST=0x00002000   // 13 - 0x0D
//-DDEFAULT_CHANLIST=0x00001000   // 12 - 0x0C
//-DDEFAULT_CHANLIST=0x00000800   // 11 - 0x0B
```

读取的信道结果，如图 3-17 所示。

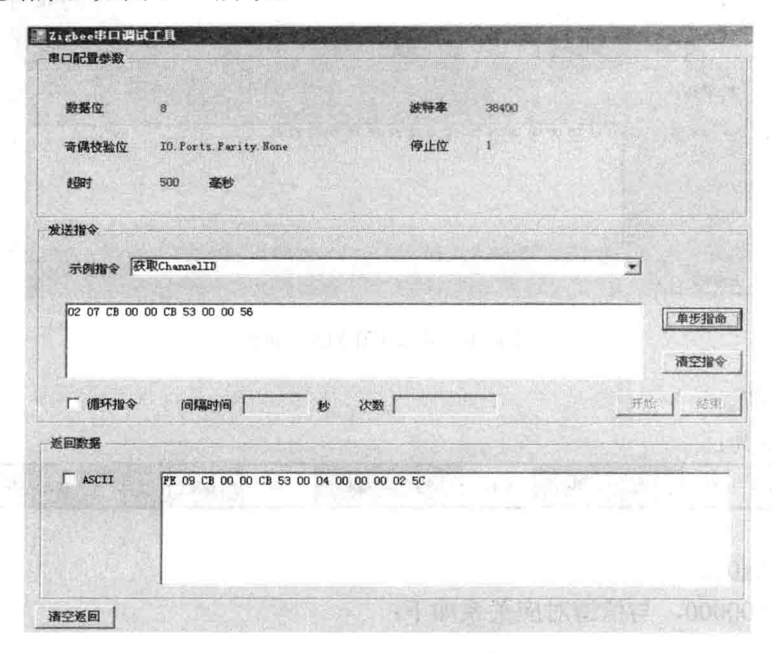


图 3-17　信道读取结果

步骤 5：获取 PANID。PC 发送 PANID 命令帧请求如下：

02	07	CB	00	00	CB	51	00	00	54

其中，

短地址 ADDR：0x0000。

终端节点号：0xCB，表示协调器节点。

ID：0x0051，表示读取 PANID。

没有数据负荷。

PC 接收数据为：

03	09	CB	00	00	CB	51	00	02	57	00	0C



其中，

数据长度：0x02。

数据：0x00FF57，表示读取到的PANID。

读取PANID结果如图3-18所示。

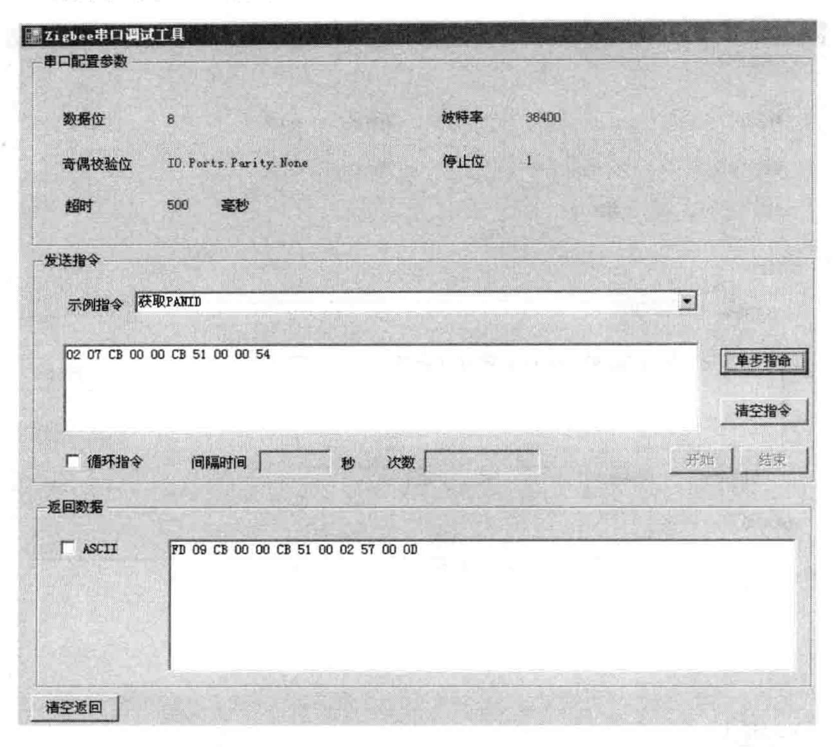


图3-18　PANID读取结果

步骤6：获取长短地址匹配。了解物理地址与网络地址匹配和格式。PC发送长短地址匹配命令帧请求如下：

02	0F	CB	00	00	D3	50	00	08	02	FF	FF	FF	FF	FF	FF	FF	C5

其中，

短地址ADDR：0x0000；//0x0000表示需要访问的节点。

终端节点号：0xCB，表示协调器。

ID：0x0050，表示长短地址匹配。

数据负荷长度为8。

长地址：FF FF FF FF FF FF FF 02。

PC接收地址匹配返回如下格式：

0C	0F	CB	3E	14	D3	50	00	08	02	FF	FF	FF	FF	FF	FF	FF	98

其中，

短地址ADDR：0x143E；//0x0001表示当前返回的短地址。

终端节点号：0xCB，表示协调器。

ID：0x0050，表示长短地址匹配。

数据负荷长度为 8。

长地址：FF FF FF FF FF FF FF 02。

长短地址匹配结果如图 3-19 所示。

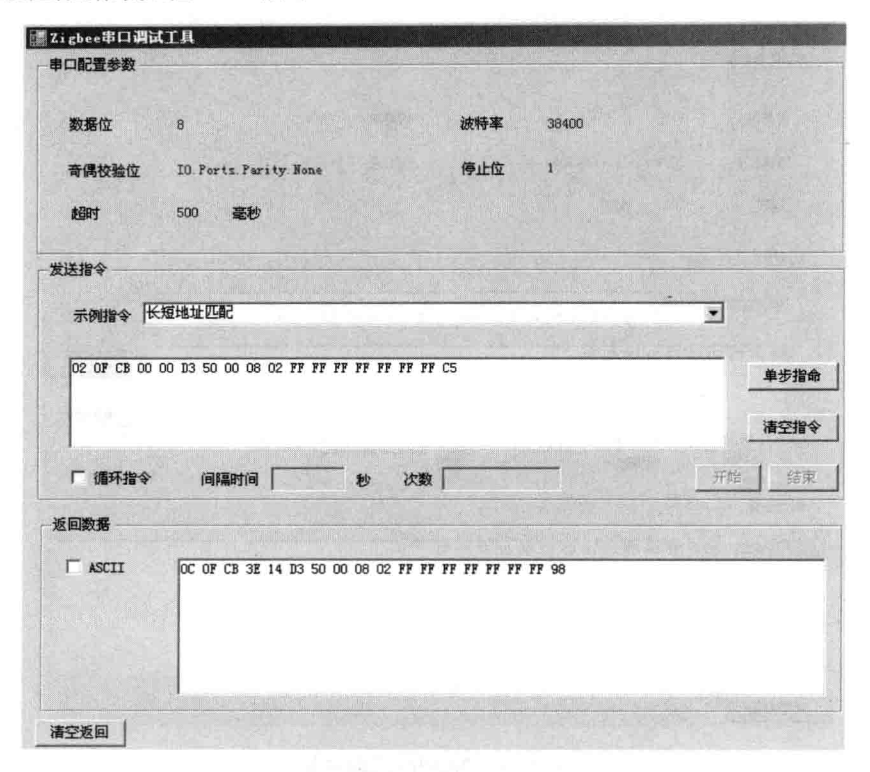


图 3-19　长短地址匹配结果

步骤 7：获取网络节点数。PC 发送网络节点数命令帧请求如下：

02	07	CB	00	00	CB	52	00	00	57

其中，

短地址 ADDR：0x0000。

终端节点号：0xCB，表示协调器节点。

ID：0x0052，表示读取节点数。

没有数据负荷。

PC 接收节点数据为：

0D	09	CB	00	00	CB	52	00	02	03	00	5A

其中，

数据长度：0x02。

数据负荷：0x0003，表示网络节点数为 2 个（不包括协调器）。

获取网络节点数界面如图 3-20 所示。



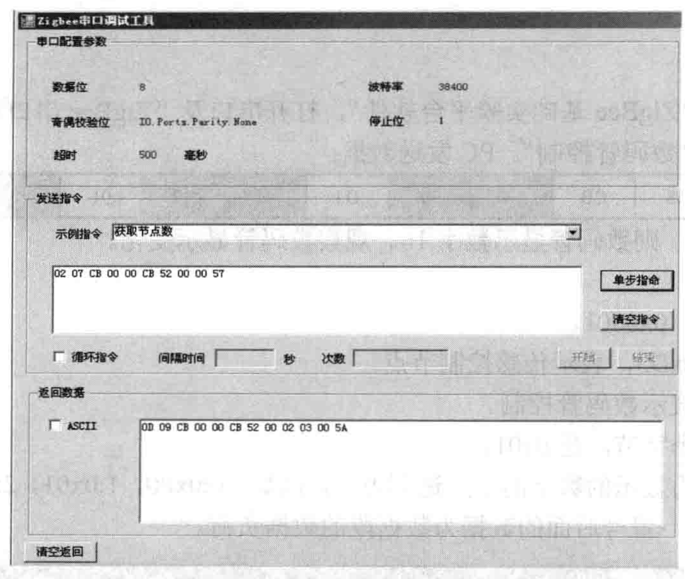


图 3-20　网络节点数显示界面

3.3.3　实训三：ZigBee 基础控制

1. 任务目标

（1）了解单片机输入/输出控制的工作原理。
（2）掌握通过 ZigBee 网络通信，利用上位软件控制各种执行器件。

2. 设备准备

（1）ZigBee 套件：协调器、传感控制节点。
（2）输入/输出控制器件：数码管模块、直流电机、步进电机。
（3）操作台：提供电源、PC、USB 口。
（4）软件：上位机软件 ZigBee 基础实验平台。

3. 星型网络拓扑结构

由协调器和传感控制节点组成的简单星型网络如图 3-21 所示。

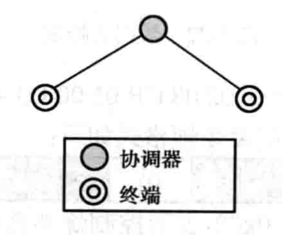


图 3-21　星型网络拓扑结构

4. 任务实施

步骤 1：运行“ZigBee 基础实验平台软件”，打开串口及“ZigBee 串口调试工具”。

步骤 2：选择“数码管控制”。PC 发送数据：

02	08	CB	01	00	D3	44	00	01	10	46

如图 3-22 所示，则数码管显示数字 16。观察数码管显示变化。

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0044，表示数码管控制。

数据负荷有一个字节，是 0x01。

数据负载格式为显示的数字的十六进制表示，例如，0:0x00，1:0x01，2:0x02……10:0x0A，11:0x0B……，其中，冒号后面的数据为数据段的数据负荷。

图 3-22　数码管控制

当设置数码管输出为 99，发送指令 02 08 CB 01 00 D3 44 00 01 63 46。

步骤 3：控制蜂鸣器。蜂鸣器控制命令帧格式如下：

02	08	CB	01	00	D3	42	00	01	00	50

如图 3-23 所示，其中数据负荷 0x00 表示控制蜂鸣器报警。此时，注意观察蜂鸣器开始鸣叫报警。



Zigbee串口调试工具
串口配置参数
数据位　8　　波特率　38400
奇偶校验位　IO.Ports.Parity.None　　停止位　1
超时　500　毫秒
发送指令
示例指令　蜂鸣器控制
02 08 CB 01 00 D3 42 00 01 00 50
单步指命
清空指令
循环指令　间隔时间　秒　次数　开始　结束
返回数据
ASCII　E6 08 CB 01 00 D3 42 00 01 00 52
清空返回

图 3-23　蜂鸣器报警

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0000，表示蜂鸣器控制。

数据负荷有一个字节，是 0x01。

数据负载 0x00 表示蜂鸣器响，0x01 表示蜂鸣器关闭。控制关闭蜂鸣器的指令：

02	08	CB	01	00	D3	42	00	01	01	50

步骤 4：（1）关闭所有的 LED 灯。选择“LED 控制”，发送指令：

02	08	CB	01	00	D3	37	00	01	FF	3B

如图 3-24 所示，则关闭所有 LED 灯。观察板载和外接 LED 灯变化。

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0037，表示 LED 控制。

数据负荷有一个字节，是 0x01。

LED 控制数据负荷为一个字节，8 位分别表示 8 个 LED 灯的状态，对应位为 0 表示亮，1 表示灭。bit0～bit3 对应板载 L5～L8，bit4～bit7 对应外接 LED 模块 LED1～LED4。

（2）打开所有 LED 灯。发送指令 02 08 CB 01 00 D3 37 00 01 00 3B，如图 3-25 所示，则打开所有 LED 灯。观察板载和外接 LED 灯状态。

图 3-24　LED 灯控制（全暗）

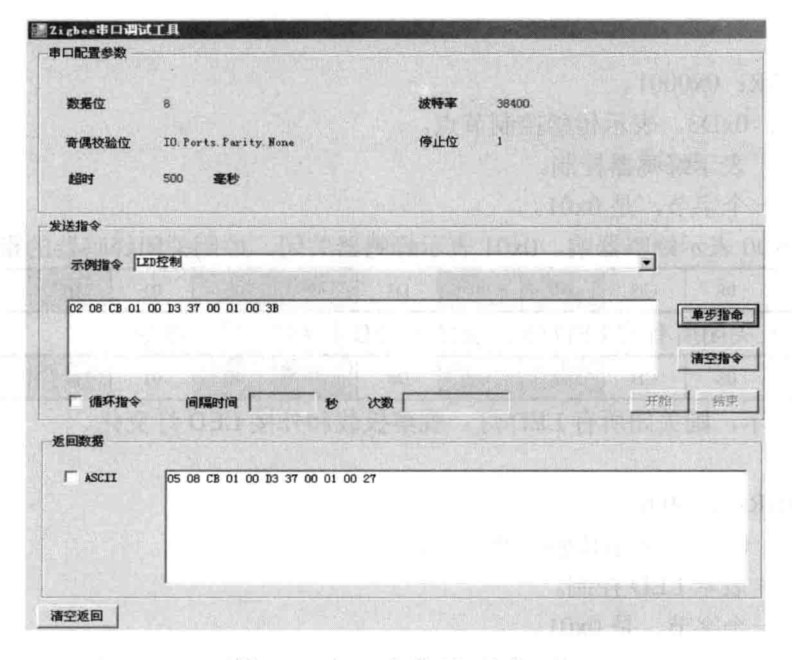


图 3-25　LED 灯控制（全亮）

（3）打开或关闭指定的 LED 灯。发送指令 02 08 CB 01 00 D3 37 00 01 IE 09，则表示板载 L5、外接 LED2～LED4 四个 LED 灯亮起，其余全暗。数据 1E，对应 8 个二进制位，每一个二进制位对应控制一个 LED 灯，如图 3-26 所示。观察板载和外接 LED 灯变化。



图 3-26　LED 灯控制

步骤 5：控制直流电机。（1）选择“电机控制”，发送控制直流电机向左转（反转）命令帧格式如下：

02	08	CB	01	00	D3	45	00	01	01	58

如图 3-27 所示。观察直流电机转动方向。

图 3-27　直流电机左转

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0045，表示直流电机控制。

数据负荷有一个字节，是 0x01，说明如下：

1	2	3	4	5	6	7	8
inB	inA	—	—	—	—	—	—

inB	inA	状态
0	0	不转
1	0	正转
0	1	反转
1	1	不转

控制直流电机右转（正转）命令格式如下：

02	08	CB	01	00	D3	45	00	01	01	58

步骤 6：控制步进电机。控制步进电机逆时针转动 360° 命令帧格式为：

02	0A	CB	01	00	D3	46	00	03	00	08	85	54

如图 3-28 所示。观察步进电机转动情况。

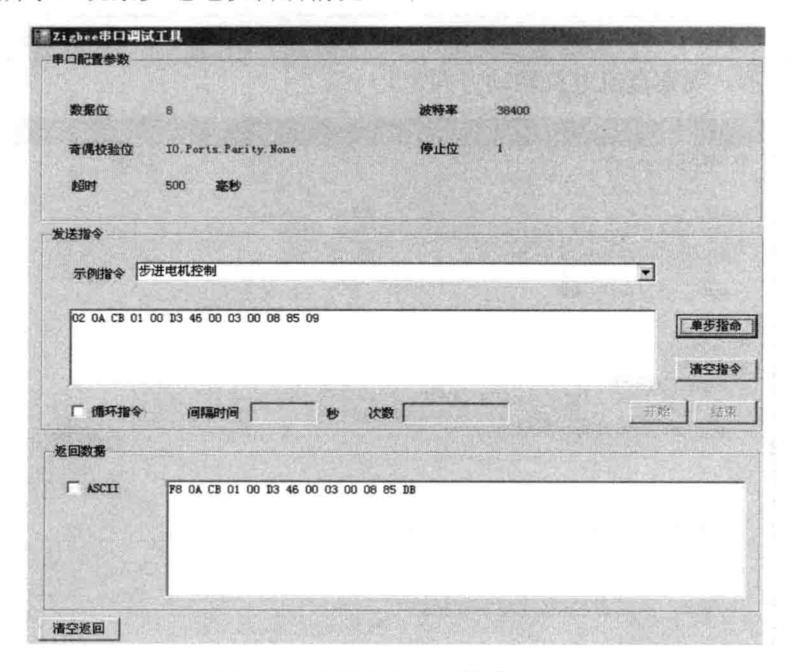


图 3-28 步进电机逆时针转 360°

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。



ID：0x0046；表示步进电机控制。

数据负荷有三个字节，是 0x03。其中，0x06 表示步进电机转动角度为 6°（参数值：0～180）；0x08 表示步进电机转动 8 个半圈（参数值：0～255）；0x00 的第 7 位表示步进电机的正反转，1 为正转，0 为反转，第 6～0 位用于设置电机转速（参数值：0～127）。

控制步进电机顺时针转动 180° 指令：02 0A CB 01 00 D3 46 00 03 00 04 05 54。

3.3.4　实训四：ZigBee 传感数据采集

1. 任务目标

采集各类传感器数据。

2. 设备准备

（1）ZigBee 套件：协调器、传感控制节点。

（2）传感器：温度、温湿度、光度、红外人体感应、烟雾、可燃气体、CO_2 等传感器。

（3）操作台：提供电源、PC、USB 口。

（4）软件：上位机软件。

3. 任务实施

步骤 1：采用板载的 DS18B20 传感器采集节点工作温度。温度传感器数据采集命令帧格式如下：

02	07	CB	01	00	D3	30	00	00	2C

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0030，表示读取温度。

没有数据负荷。

接收温度数据为：

01	09	CB	01	00	D3	30	00	02	49	01	6A

则返回温度数据负荷为 0x0149。其中，数据：0x0149，表示＋20.56℃。温度数据格式参考 DS18B20 格式。

利用板载的 DS18B20 传感器采集节点工作温度，并对采集结果进行分析，如图 3-29 和图 3-30 所示。也可以采用附录一中换算方法。

步骤 2：采用 SHT10 温湿度传感器，采集环境温度和湿度。将 SHT10 温湿度传感器模块 CH-SM-SHT 连接在 ZigBee 传感控制节点温湿度传感器接口上进行数据采集。

（1）温湿度传感器采集温度命令帧格式为：

02	07	CB	01	00	D3	36	00	00	2A

图 3-29　DS18B20 温度传感数据采集

图 3-30　DS18B20 温度采集结果分析

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0036，表示读取 SHT10 传感器温度。

没有数据负荷。

接收温度数据为：

02	09	CB	01	00	D3	36	00	02	C7	16	F5



返回外接温度数据负荷为0x16C7。其中，数据：0x16C7，温湿度数据格式参考SHT10格式。发送温度采集指令，并对采集结果进行分析，如图3-31所示。

图3-31　SHT10温度数据采集

（2）温湿度传感器采集湿度命令帧格式为：

02	07	CB	01	00	D3	31	00	00	09

其中，

短地址ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0031，表示读取SHT10传感器湿度。

没有数据负荷。

接收湿度数据为：

02	09	CB	01	00	D3	31	00	02	4B	06	75

其中，数据：0x064B，温湿度数据格式参考SHT10格式。发送湿度采集指令，并对采集结果进行分析，如图3-32和图3-33所示。

步骤3：光敏传感器采集数据。02 07 CB 01 00 D3 32 00 00 2E。

（1）板载光照度数据采集命令帧格式为：

02	07	CB	01	00	D3	32	00	00	2E

其中，

短地址ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0032；表示读取板载光照度。

没有数据负荷。

图 3-32　SHT10 湿度数据采集

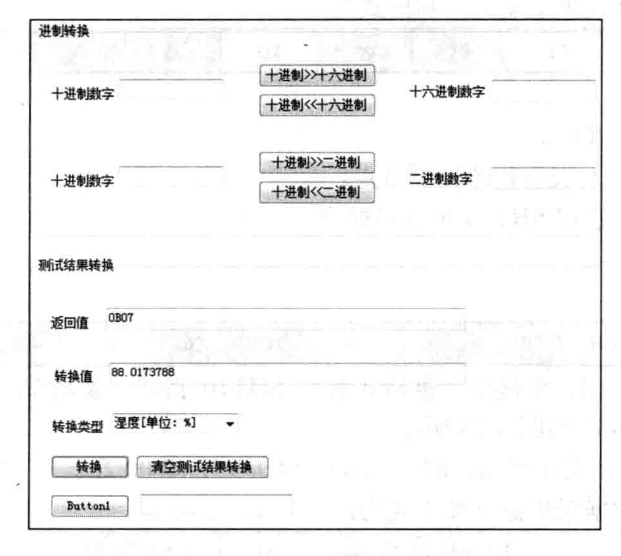


图 3-33　SHT10 湿度采集结果分析

接收光照度数据为：

07	09	CB	01	00	D3	32	00	02	E4	62	A5

返回板载光照数据负荷：0x62E4。

利用测试结果转换工具，将返回数据转换成实际光照度值。具体转换公式可参考光敏传感器介绍，如图 3-34 和图 3-35 所示。



图 3-34　板载光照度数据采集

图 3-35　板载光照度结果分析

（2）外接光敏传感器数据采集命令帧格式为：

02	07	CB	01	00	D3	34	00	00	28

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0034，表示读取外接光敏传感器或气体传感器。

没有数据负荷。

接收数据为：

22	09	CB	01	00	D3	34	00	02	18	50	6E

返回外接光照数据负荷为 0x5018。

利用测试结果转换工具，将返回数据转换成实际温度值，如图 3-36 和图 3-37 所示。具体转换公式可参考光敏传感器介绍。

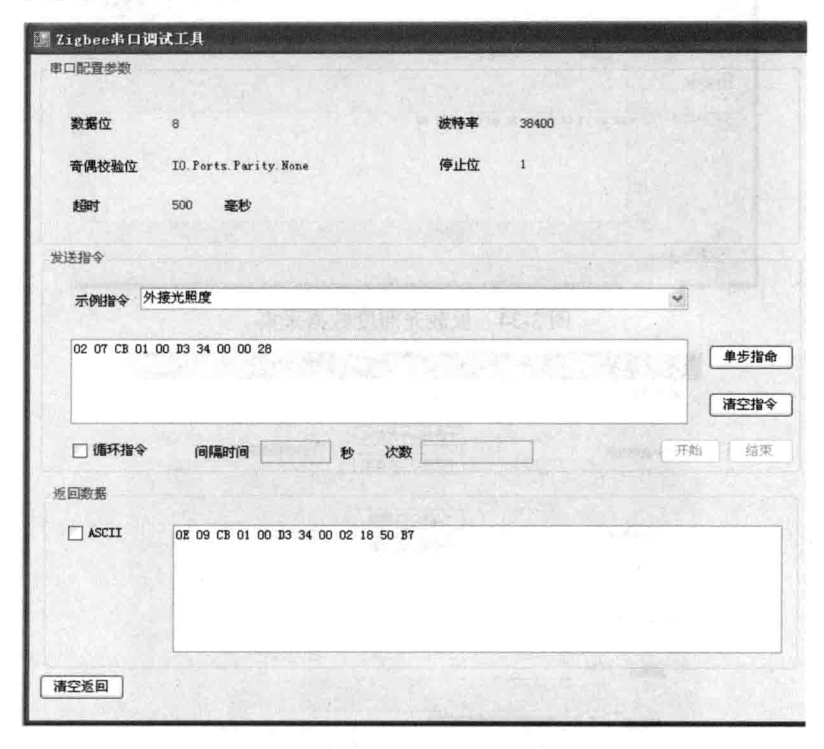


图 3-36 外接光照度数据采集

步骤 4：烟雾传感器采集数据。烟雾传感器数据采集命令帧格式为：

02	07	CB	01	00	D3	29	00	00	35

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0034，表示读取外接光敏传感器或气体传感器。

没有数据负荷。

接收数据为：

07	09	CB	01	00	D3	29	00	02	58	21	42

则返回烟雾探测数据负荷为 0x2158。



图 3-37　外接光照度采集结果分析

利用测试结果转换工具，将返回数据转换成烟雾浓度值，如图 3-38 和图 3-39 所示。具体转换公式可参考 MQ2 烟雾探测传感器介绍。

图 3-38　烟雾检测数据采集

图 3-39　烟雾浓度检测结果分析

步骤 5：可燃气体传感器采集数据。可燃气体传感器数据采集命令帧格式如下：

02	07	CB	01	00	D3	49	00	00	55

其中，

短地址 ADDR：0x0001。

终端节点号：0xD3，表示传感控制节点。

ID：0x0049，表示读取外接气体传感器。

没有数据负荷。

接收数据为：

07	09	CB	01	00	D3	49	00	02	F8	28	8B

返回可燃气体数据负荷：0xF828。

利用测试结果转换工具，将返回数据转换成可燃气体浓度值，如图 3-40 和图 3-41 所示。具体转换公式可参考 MQ5 可燃气体传感器介绍。

步骤 6：CO_2 传感器采集数据。用打火机中的燃气对照燃气探头片刻，然后再采集数据。如图 3-42 所示，返回数据负荷为 0x7CC0。



图 3-40　可燃气体数据采集

图 3-41　可燃气体浓度检测结果分析

利用测试结果转换工具，将返回数据转换成可燃气体浓度值，如图 3-43 所示。

图 3-42 可燃气体检测

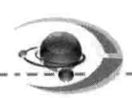
图 3-43　测试结果分析

步骤 7：红外人体感应传感数据采集。红外人体感应数据采集命令帧格式如下：

02	08	CB	01	00	D3	33	00	01	0A	2B

其中，

短地址 ADDR：0x0001。



终端节点号：0xD3，表示传感控制节点。

ID：0x0033，表示读取红外感应器状态。

数据长度：0x01。

数据为定时器间隔，如果数据不等于 0x00，则节点打开红外采集，并定时发送采集状态。如果数据等于 0x00，则关闭红外采集。

接收红外感应器采集数据为：

38	08	CB	01	00	D3	33	00	01	00	23

数据负荷为 0x00，表示无干扰状态，如图 3-44 所示。

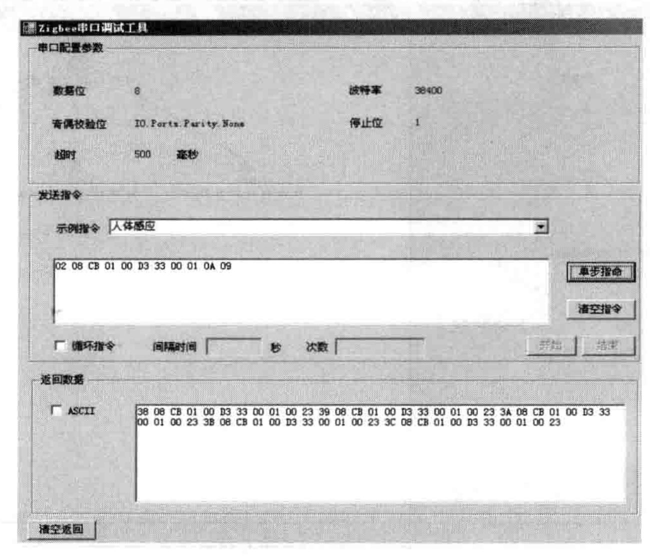


图 3-44　红外人体感应采集

若此时在人体感应传感器附近有人体移动，则返回数据如图 3-45 所示。

图 3-45　人体感应（有人）

发送人体感应指令 02 08 CB 01 00 D3 33 00 01 00 2B，则停止人体感应状态采集。

3.4 练习题

1．依次打开 ZigBee 协调器和传感控制节点后，建立 ZigBee 网络，生成图 3-46 所示简单星形网络拓扑结构。

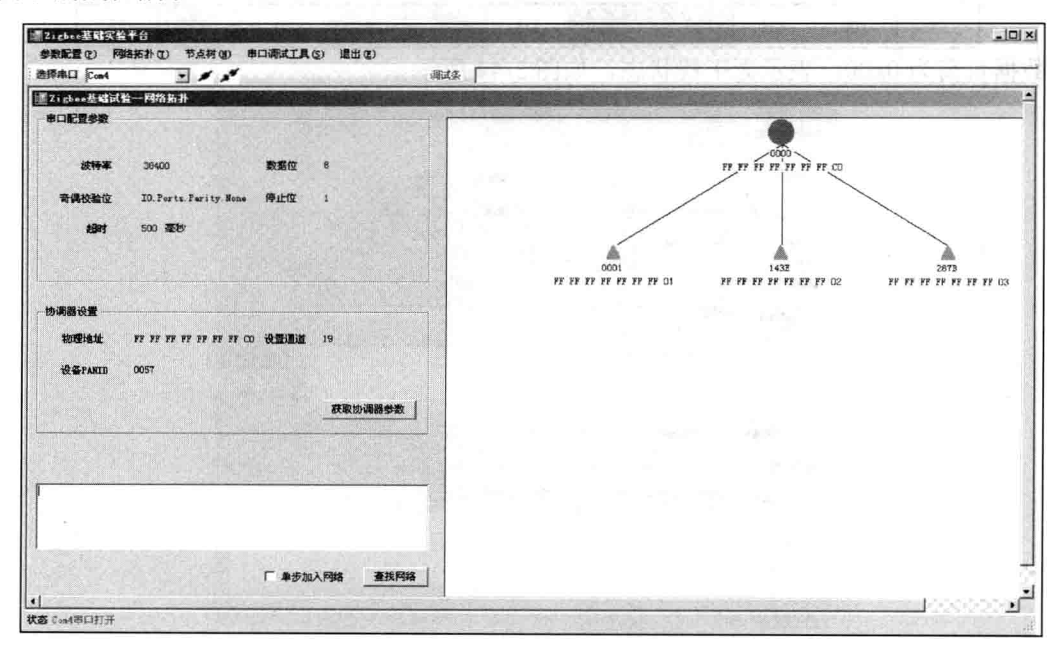


图 3-46　ZigBee 网络节点图

根据图 3-46 和图 3-47 对应关系，将协调器和节点的地址填入下面空白处。

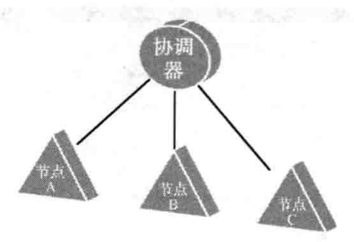


图 3-47　图 3-46 中网络拓扑结构

协调器：网络地址：____________________；MAC 地址：____________________。
长地址：____________________；短地址：____________________。
节点 A：网络地址：____________________；MAC 地址：____________________。
长地址：____________________；短地址：____________________。
节点 B：网络地址：____________________；MAC 地址：____________________。
长地址：____________________；短地址：____________________。



节点 C：网络地址：______________；MAC 地址：______________。

长地址：______________；短地址：______________。

2．为了获得协调器的 MAC 地址，发送的指令是：______________；返回的数据是：______________；MAC 地址是：______________。

3．为了获取 Channel ID 值，发送的指令是：______________；数据负荷为：______________；Channel ID 值是：__________；信道为：__________。

4．为了获取 PANID 值，发送的指令是：______________；数据负荷为：______________；PANID 值是：__________。

5．为了获取节点数，发送的指令是：______________；数据负荷为：______________；节点数为：__________。

6．为读取板载 DS18B20 温度，发送指令：02 07 CB 01 00 D3 30 00 00 2C，返回数据如图 3-48 所示。

则返回温度数据负荷为 0x__________。

请根据“附件一”计算出板载温度：__________。

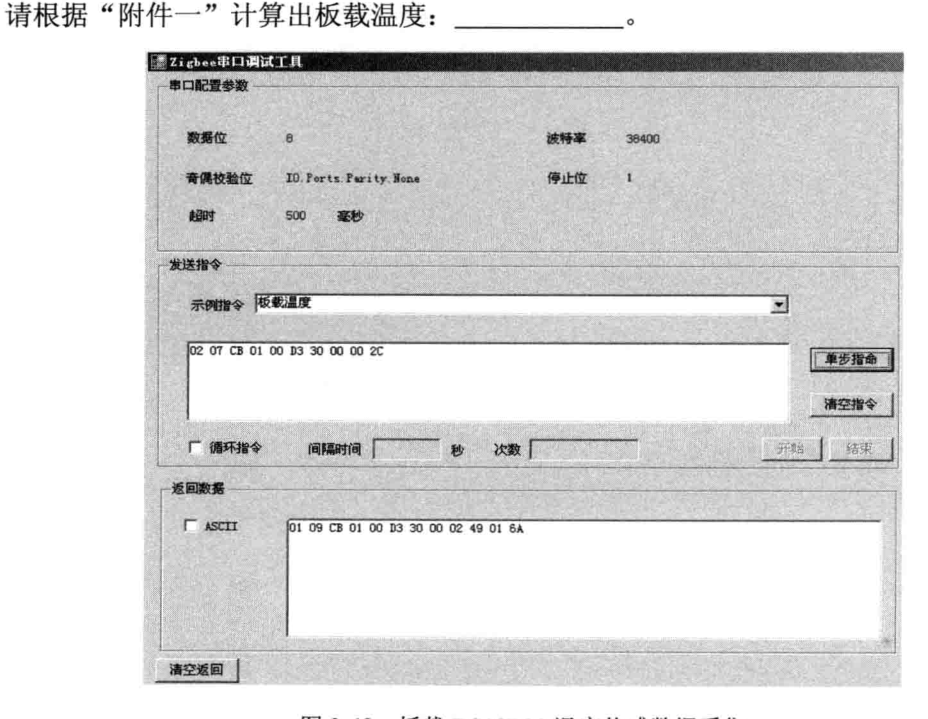


图 3-48　板载 DS18B20 温度传感数据采集

7．采用光敏传感器，采集板载光照度。发送指令：______________；返回数据为：______________；数据负荷为：0x________；利用测试结果转换工具，将返回数据转换成实际光照度值为：__________。

8．请填写下列控制命令已实现各项功能。

（1）通过控制命令：______________控制直流电机转动。

（2）通过控制命令：______________控制直流电机停止。

（3）通过控制命令：________________________控制步进电机转动。

（4）通过控制命令：________________________控制直流电机停止。

（5）通过控制命令：________________________控制外接 LED 灯第 2 个灯开。

（6）通过控制命令：________________________控制外接 LED 灯第 2 个灯关。

（7）通过控制命令：________________________控制第 3 节点的板载 LED 灯开。

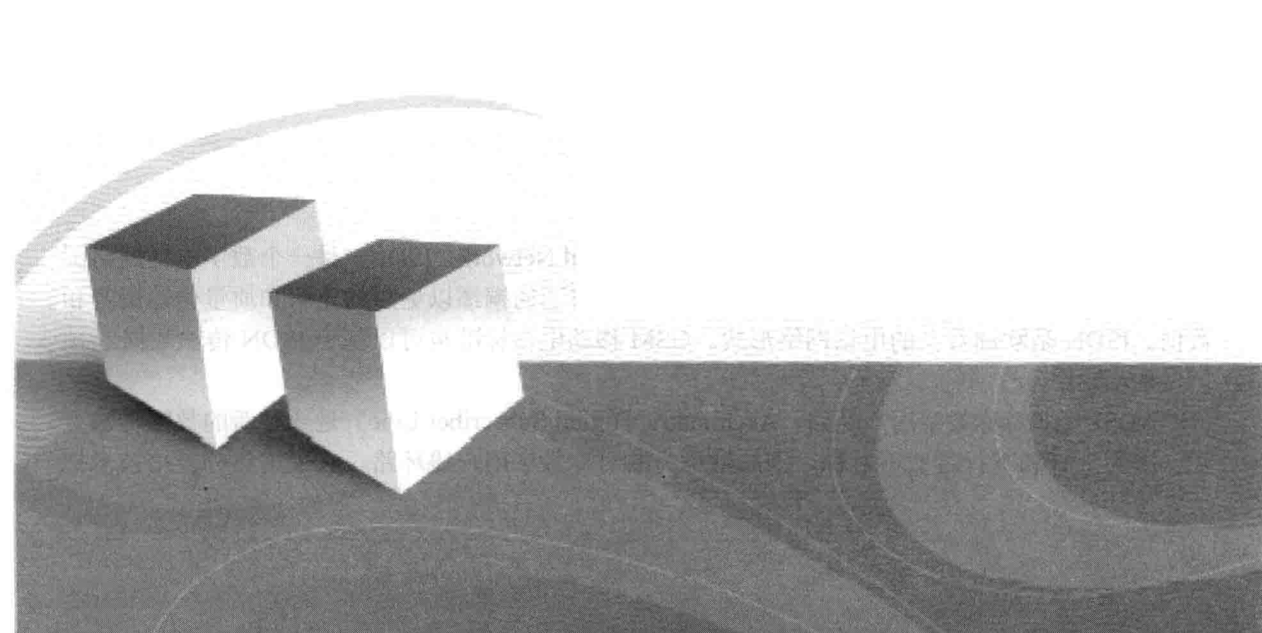
（8）通过控制命令：________________________控制第 3 节点的板载 LED 灯关。

（9）通过控制命令：________________________控制数码管（将温度设置为 36℃）。

第4章

物联网无线通信技术

网络是物联网重要的基础设施之一，无线网络在物联网中扮演重要角色。本章学习的目的是了解网络通信的基本概念和技术，深入探讨蓝牙（Bluetooth）、WiFi 和 GPRS 技术的应用和操作方法。



4.1 互联网简述

互联网是成千上万信息资源的总称，这些资源以电子文件的形式，在线分布在世界各地的计算机上；互联网上开发了许多应用系统，供接入网上的用户使用，网上的用户可以方便地交换信息，共享资源。互联网是各种使用 TCP/IP 协议互相通信的数据网络的集合。

4.1.1 互联网基本组件

1. 网络接入方式

网络终端包含了个人计算机、服务器、笔记本、手机、iPad、iPhone 以及贴附 RFID 标签的物品和无线传感器等。从连接关系上看，之所以称其为网络终端是因为这些设备是通过某种接入方式从网络的边界处接入网络的。只要设备从网络的边界上成功地接入网络，就具有了和已经存在于网络上的其他设备通信的能力。

虽然互联网给终端设备提供了友好的接口，但由于终端设备的多样性，如果想将设备真正接入网络，还有一些问题亟待解决。似乎很难有一种通用的接入方式。例如，个人计算机和服务器体积比较大，可以通过有线的方式将其与互联网相连。但是，手机和 PDA 呢，也要给它们一根网线来上网吗？还有贴附着 RFID 标签的物体呢？标签本身的体积可能比网线的接口还小，到底要做何处理？为了解决这些问题，人们设计了多种针对设备特点的网络接入方式，每一种接入方式考虑到设备体积和处理能力，找到一种合适的方式接入互联网。

互联网接入技术大致分为 3 种类型。

- 拨号接入。通过拨号方式将主机与互联网连接，常用于家庭住宅主机上网使用，如 ISDN、ADSL 和 Cable Modem 等。
- 局域网接入。将局域网上的主机与互联网连接，常用于公司和大学校园主机上网使用。
- 无线接入。将手机、笔记本、iPad 等移动终端通过无线链路与互联网连接。

用户选择接入方式时，需要考虑用户所处的位置和通信条件、使用者数量、通信量、希望访问的资源、要求响应的速度、设备条件以及资金投入等因素，下面介绍我国使用的几种接入互联网的方式。

（1）拨号接入。

拨号接入技术主要包括以下几种。

- ISDN

ISDN 综合业务数字网（Integrated Services Digital Network，ISDN）是一个数字电话网络国际标准，是一种典型的电路交换网络系统。它通过普通的铜缆以更高的速率和质量传输语音和数据。ISDN 是欧洲普及的电话网络形式。GSM 移动电话标准也可以基于 ISDN 传输数据。

- ADSL

ADSL（非对称数字用户环路，Asymmetric Digital Subscriber Line）是一种新的数据传输方式。因为上行和下行带宽不对称，因此被称为非对称数字用户线环路。它采用频分复用技术把



普通的电话线分成了电话、上行和下行三个相对独立的信道，从而避免了之间的相互干扰。即使边打电话边上网，也不会发生上网速率和通话质量下降的情况。通常 ADSL 在不影响正常电话通信的情况下可以提供最高 3.5Mbit/s 的上行速度和最高 24Mbit/s 的下行速度。

使用 ADSL，需在用户线两端各安装一个 ADSL 调制解调器（见图 4-1），该调制解调器采用了频分多路复用（Frequency-division Multiplexing，FDM）技术，将带宽分为 3 个频段部分。图 4-2 所示为 ADSL 电话线上的带宽分配图。PSTN 为一般语音通话使用，Upstream 为 ADSL 上行频段，Downstream 为 ADSL 下行频段。

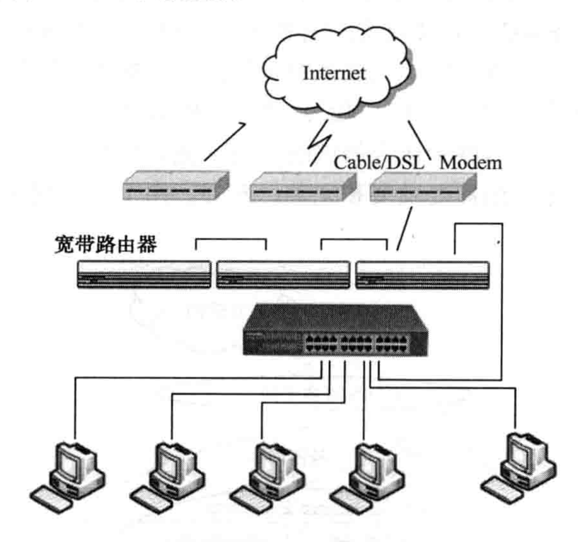


图 4-1 ADSL 结构图

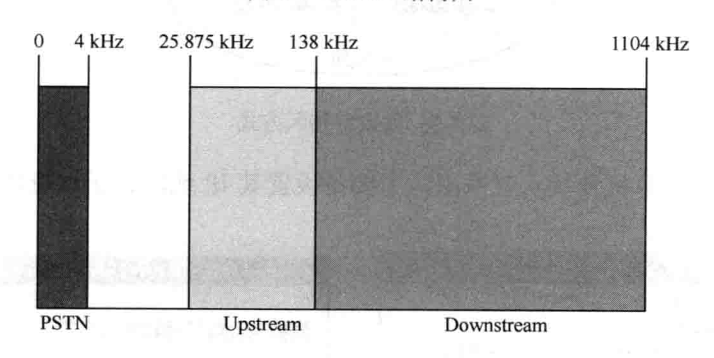


图 4-2 ADSL 频率分配图

由于受到传输高频信号的限制，ADSL 需要电信服务提供商端接入设备和用户终端之间的距离不能超过 5 千米，也就是用户的电话线连到电话局的距离不能超过 5 千米。

● Cable Modem

Cable Modem 是一种可以通过有线电视网络进行高速数据接入的装置。它一般有两个接口，一个用来接室内墙上的有线电视端口，另一个与计算机相联。Cable Modem 不仅包含调制解调部分，它还包括电视接收调谐、加密解密和协议适配等部分，它还可能是一个桥接器、路由器、网络控制器或集线器。一个 Cable Modem 要在两个不同的方向上接收和发送数据，把上、下行

数字信号用不同的调制方式调制在双向传输的某一个 6MHz（或 8MHz）带宽的电视频道上。它把上行的数字信号转换成模拟射频信号，类似电视信号，所以能在有线电视网上传送。接收下行信号时，Cable Modem 把它转换为数字信号，以便计算机处理。

Cable Modem 的传输速度一般可达 3Mbit/s～50Mbit/s，距离可以是 100 千米甚至更远。

（2）以太网。

以太网是应用最为广泛的局域网通信技术，它的接入利用了以太网具有的简单、低成本、可扩展性强、与 IP 网络和业务事例性好等特点，对学校、公司等单位用户来说，以太网是一种主流的网络接入方式（见图 4-3）。以太网包括标准的以太网（10MB/s）、快速以太网（100MB/s）和 10G（10GB/s）以太网，可以实现不同速率的宽带接入，提供高速的局域网及高速的互联网服务。用户只需要一台带有网络接口卡（NIC）的计算机即可上网。但是由于以太网本质上是一种局域网技术，用于公用电信网的接入领域时，在认证计费和用户管理、用户和网络安全、服务质量控制、网络管理等方面需要发展和完善；此外，由于以太网接入需要进行综合布线，初期投资成本比较高。

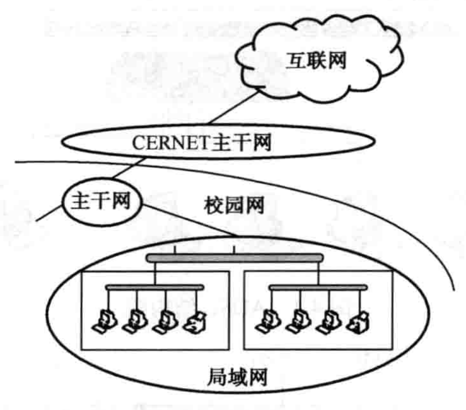
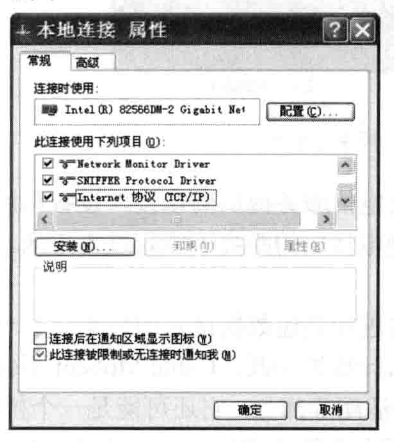


图 4-3　以太网接入方式

在局域网内部的计算机要接入互联网，主要是设置其 IP 地址、子网掩码、网关和 DNS 服务器，如图 4-4 所示。



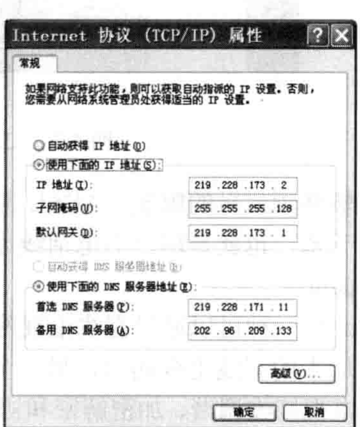


图 4-4　局域网连接属性设置



（3）无线接入。

无线接入是继有线接入之后发展起来的另一种互联网的接入方式，借助无线接入技术，无论在何时、何地，人们都可以轻松地接入互联网。常用无线接入方式在结构上大致分为两种类型：一种是局端设备之间通过无线方式互联，相当于中继器，如图 4-5 所示；另一种是用户终端采用无线接入方式接入局端设备，如图 4-6 所示。

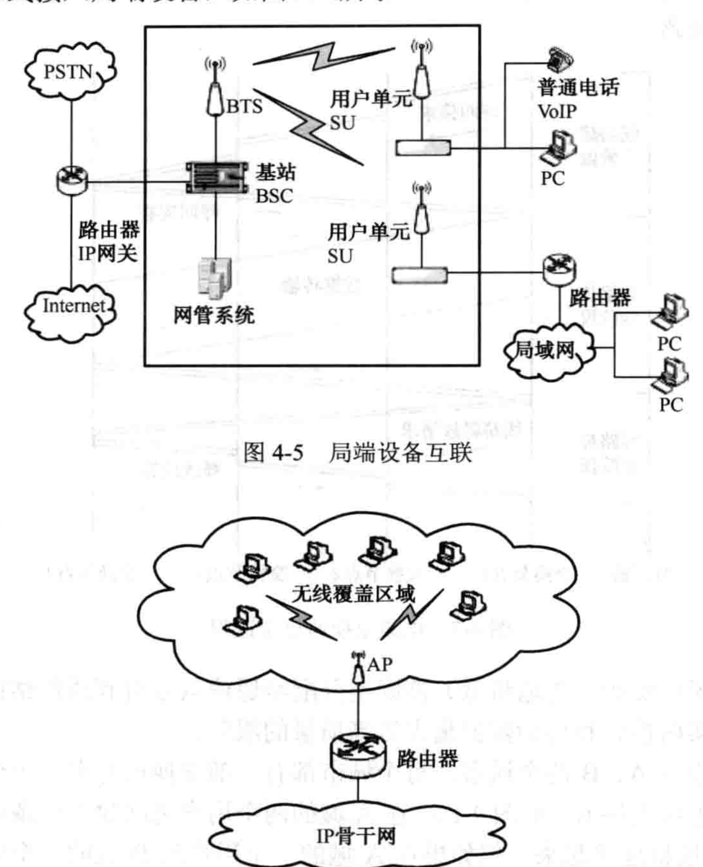


图 4-5　局端设备互联

图 4-6　终端到局端设备互联

2. 网络交换技术

前面已经了解了网络终端的概念以及主流的网络接入方式，但是对于互联网内部究竟是如何提供通信服务的还一无所知。换句话说，当一个网络终端设备发送出一个数据包给另一个网络设备，两者在地理位置上可能位于地球的两端。如此遥远的距离，网络上可能有上亿个终端同时在线。那么互联网究竟是如何保证数据包准确地从发送端传递到接收端的呢？沿着之前由外至内的讨论方式，从这里走进互联网这个黑盒子内部，探其究竟。

在网络中，将数据从发送端发送到接收端接收的过程称为数据交换。按照交换方式的不同，数据交换可以分为 3 种：电路交换、报文交换和分组交换。其中分组交换又包含虚电路和数据报两种子模式。这里讨论两种主流的数据交换模式：电路交换和分组交换中的数据报模式。

（1）电路交换。

当用户之间要传输数据时，控制中心会在网络之中为通信的双方建立一条暂时的数据电路（circuit）。在使用电路交换打电话之前，先拨号建立连接（见图 4-7）。当用户听到“嘟……嘟……嘟”的接通音的时候，表明电路建立完毕。电路接通后，用户双方便可通过已建立起的电路进行数据传输，并一直占用到传输完毕。通话结束挂机后，挂机信令告诉这些交换机，使交换机释放刚才这条物理通路。

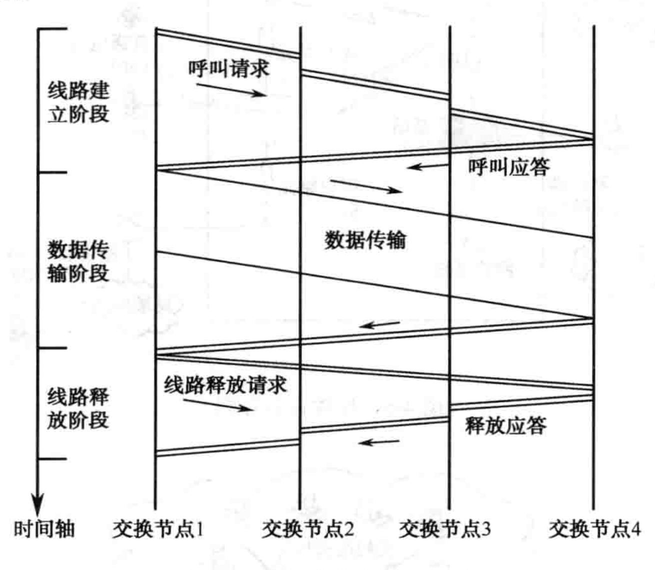


图 4-7　电路交换通信全过程

由于网络中的通信资源（传输带宽）被固定分配给通信双方直到通信结束，因此电路交换提供延时小、传输实时性强和传输数据量大等高质量的服务。

举例来说，假设有 A、B 两个城市，每个城市都有一部交换机并有一千个用户，两个交换机之间用 100 条中继线连接着（见图 4-8）。在 A 城的两个用户之间建立一条电路是指两条用户线路通过 A 城的交换机连接起来。但如果在 A 城的一个用户和 B 城的一个用户之间建立一条电路时，人们指的就是由 A 城的用户线路经 A 城交换机连接到 A、B 城之间的一条中继线路，再经 B 城交换机连接到 B 城的用户线路上。由于经济上的原因，中继线路总是大大少于用户线路，并且为所有用户所共享。那么，当人们占用了一条中继线路以后，即使不传送信息，别人也不能使用，因此电路空闲时间占大约 50%，这就是电路交换最主要的缺点。

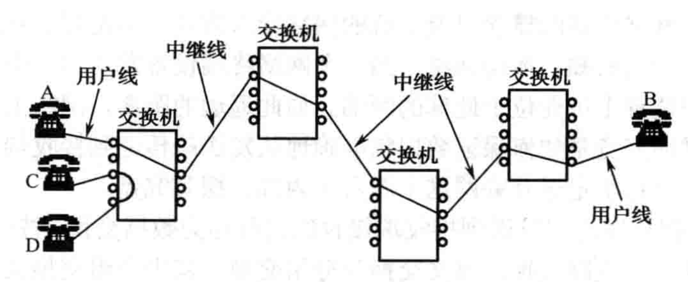
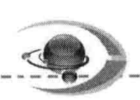


图 4-8　电路交换通信连接图



（2）分组交换。

分组交换是将数据以分组为单位在网络中进行传输，始于1970年。当前两种最新的广域网技术：帧中继和ATM，基本上是分组交换方式的变种。

分组交换有两种方式。

① 数据报方式：在这种方式中，每个分组按一定格式附加源与目的地址、分组编号、分组起始、结束标志、差错校验等信息，以分组形式在网络中传输。网络只是尽力地将分组交付给目的主机，但不保证所传送的分组不丢失。如图4-9（a）所示，主机H1向H5发送的分组，有的经过节点A—B—E，有的经过A—C—E或A—B—C—E；主机H2向H6发送的分组，有的经过节点B—D—E，有的经过B—E。数据报方式的优点是传输延时小，当某节点发生故障时不会影响后续分组的传输。缺点是每个分组附加的控制信息多，增加了传输信息的长度和处理时间，增大了额外开销。

② 虚电路方式：它与数据报方式的区别主要是在信息交换之前，需要在发送端和接收端之间先建立一个逻辑连接，然后才开始传送分组，所有分组沿相同的路径进行交换转发，通信结束后再拆除该逻辑连接。网络保证所传送的分组按发送的顺序到达接收端。所以网络提供的服务是可靠的，也保证服务质量。如图4-9（b）所示，主机H1向H5发送的所有分组都经过相同的节点A—B—E，主机H2向H6发送的所有分组也都经过相同的节点B—E。

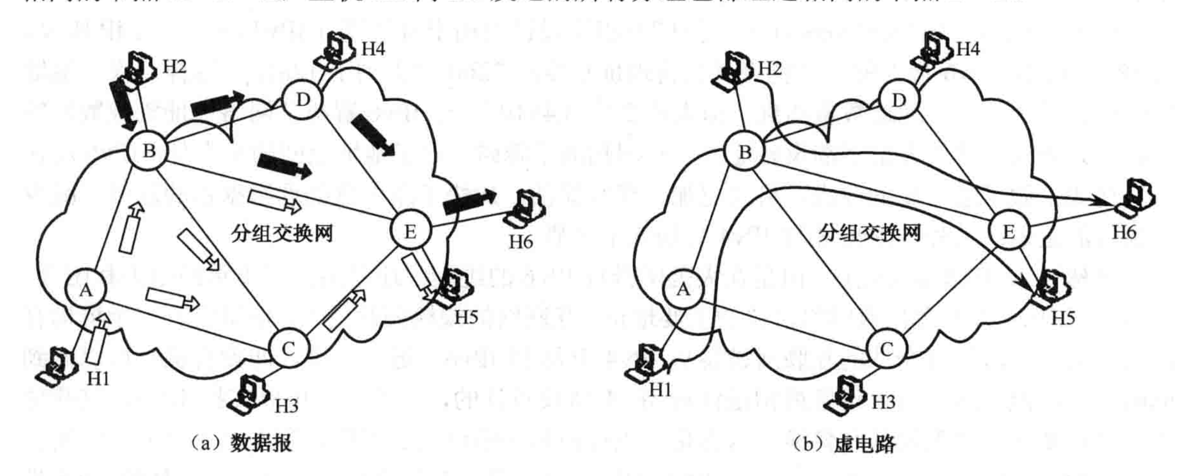


图4-9　分组交换

分组交换网与电路交换网相比有许多优点：

① 线路利用率更高。因为结点到结点的单个链路可以由很多分组动态共享。

② 分组交换网可以实行两个不同数据传输率的站之间能够交换分组，因为每一个站以它自己的数据率连接到这个结点上。

③ 排队制。当电路交换网上负载很大时，一些呼叫就被阻塞了。在分组交换网上，分组仍然被接受，只是其交付时延会增加。

④ 支持优先级。在使用优先级时，如果一个节点有大量的分组在排队等待传送，它可以先传送高优先级的分组。这些分组因此将比低优先级的分组经历更少的时延。

由于分组交换的以上优点，可以预见在物联网时代，分组交换依旧会成为主流的数据交换

方式。在物联网中，巨大数量的网络终端将会被连接在网络上，如果采用电路交换，以现有互联网的容载能力，很难支撑起如此巨大的网络通信开销。分组交换不能保证服务质量的缺陷可以通过其他一些方式进行补偿，最终实现具有高质量保证的传输。另外，在很多情况下，物联网的服务不必苛求具有延迟保障的即时通信能力。因此，高效并且低成本的分组交换必然会成为物联网中数据交换的首选方式。

4.1.2 从互联网到物联网

1. IPv4 向 IPv6 过渡

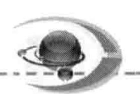
在互联网中，每一个网络终端拥有一个唯一的身份号码：IP 地址。虽然 IPv4 仍是当前的主流，但是 IPv4 地址长度为 32bit，这意味着 IPv4 可以支持最大数量不同的 IP 地址只有 2^{32}=4.3×10^{9}个，随着接入网络终端数量的剧增，IPv4 的网络地址面临枯竭的局面。北美占有绝大多数的 IP 地址资源，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国只有 3000 多万个。IP 地址不足严重地制约了互联网的应用和发展。为了突破 IPv4 地址限制的壁垒，新的解决方案 IPv6 应运而生。

IPv6（Internet Protocol Version 6）是 IETF 组织设计的用于替代现行 IPv4 的下一代 IP 协议。与 IPv4 相比，IPv6 最大的一个特点就是将地址长度从 32bit 增大到了 128bit。这样一来，地址空间增大了 296 倍，地址数量达到了惊人的 2^{128}=3.4×10^{38} 个。IPv6 解决了网络地址资源数量的问题，为物联网时代大量终端设备连入互联网扫清了障碍。除了地址空间的扩大外，IPv6 还在包头格式上做了进一步的改进，格式更加合理和简洁，加快了路由器处理数据包的速度，减少了通信的延迟。另外，IPv6 相比 IPv4 更加安全可靠。

虽然 IPv6 有诸多的优点，但是在大范围推行 IPv6 的进程中还是遇到了重重的阻力和困难。原因在于 IPv4 依旧占据着网络协议的主要地位，互联网的规模如此巨大，使得没有一个机构有能力在同一个时间将全球的互联网设备从 IPv4 升级到 IPv6。退一步讲，即使有机会可以做到同时升级，但网络中很多设备最初是针对 IPv4 协议设计的，并不一定可以支持 IPv6，这些位置上的设备必须重新设计和替换，这将是一项规模和开销巨大的工程，基本上不可能短时间在全球范围内完成更新。因此，IPv4 到 IPv6 的过渡必须是一个循序渐进的过程，在体验 IPv6 带来的好处的同时仍能与网络中其余的 IPv4 用户通信。能否顺利地实现从 IPv4 到 IPv6 的过渡也是 IPv6 能否取得成功的一个重要因素。

2. 互联网向物联网延伸

当 IPv6 有能力为地球上每一个用户分配一个 IP 地址时，人们自然憧憬一个新时代的到来——物联网时代。无论是在当下还是在下一代互联网中，可预见到"联"在网络上的设备主要还是计算机、PDA、手机等依赖人类操作的电子设备，难以摆脱"人在上网"的束缚。物联网的到来，特别是终端设备的多元化，将会为互联网带来延伸和拓展。物联网的时代，联网终端扩展到了所有可能的物品。以前，游离在网络之外的物品，如电视、电冰箱、电灯等，现在都可能成为网络的一分子。物联网将过去虚拟的网络世界和现在的物理世界紧密地连接在了一



起。另一方面，在互联网时代，获取信息更多的是依靠用户主动地在网络上搜寻信息；而在物联网时代，得益于传感器技术和无线射频识别技术的迅速发展，当物品结合传感器节点或者RFID 标签之后，人们不仅可以主动获取数据，还将会随时被告知自己感兴趣的物体或人的信息，方便进一步的处理和控制，以达到信息获取多样化和感知行为智能化。另外，物体之间在空间上的距离很大程度上通过它们在网络上的互联而被缩减。人与物更加紧密地联系在一起，人类对于物理世界的控制能力将得到前所未有的加强。

物联网是现有互联网的拓展，特别是在网络接入设备和方式上。大量异构设备，通过有线或者无线的方式，采用适当的标准通信协议，接入互联网。物联网的末梢是传感器和 RFID 等自动信息获取设备，也包括传统的互联网终端（例如个人计算机）；物联网核心网络是互联网或者说是作为互联网基础设施的电信网络。互联网技术进一步为物联网提供应用平台和技术支撑。反过来，物联网上的新型应用也会促进互联网的发展。

4.2 无线宽带网络

21 世纪以来，移动设备（iPhone、iPad、笔记本电脑等）与日俱增，其数量已逐渐超过了固定设备（台式机、服务器等）。如何将这些移动设备稳定、高速地联入互联网中呢？无线宽带技术（WiFi、WiMAX 等）在其中起到了至关重要的作用。无线宽带网络消除了有线网络对接入设备的位置限制，同时也节省了相应的光纤、电缆等有线信号传输设施的成本。这就意味着人们要以相对低廉的价格，非常方便地使用手机或无线上网设备在图书馆、商场、餐厅、机场、火车站、教学大楼等任何有无线信号覆盖的区域上网浏览、获取信息。物联网要做到世界上任何物体皆有址可循，如大到油轮、火车、飞机，小到温度/湿度/压力传感器、微处理器、微控制器都将被连成一个整体。并且物联网将物理世界和信息世界归一化，从信息的采集，到决策的制定和执行要一体化，因此更高速、更可靠、更廉价及更普及的点对点互联、信息传输手段是物联网所必需的。以覆盖范围较广、传输速度较快为特点的无线宽带技术势必将在物联网时代扮演重要角色。

4.2.1 无线网络基本元素

无线网络包含了一系列无线通信协议。例如蓝牙、WiFi、WiMAX、GPRS（2.5G）和 3G 协议等。为了更准确地区别不同协议的特性，需要明确一些组成无线网络的基本元素。

（1）无线网络用户。指具备无线通信能力，并可将无线通信信号转化为有效信息的终端设备。如，装有 WiFi 无线模块的台式机、笔记本电脑或 PDA，装有 GSM、GPRS 和 3G 通信模块的手机、iPad 和装有 CC2420 无线通信模块的传感器等。

（2）无线连接。无线连接是指无线网络用户与基站或者无线网络用户之间用以传输数据的通路。它主要通过无线电波、光波作为传输载体。不同无线连接技术提供了不同的数据传输速率和传输距离。

（3）基站。基站将一些无线网络用户连接到更大的网络中（如校园网、互联网或电话网等），如图 4-10 所示。无线网络用户通过基站接收和发送数据包，基站将用户的数据包转发

给它所属的上层网络，并将上层网络的数据包转发给指定的无线网络用户。根据不同的无线连接协议，相应基站名称和覆盖范围是不同的。例如，WiFi 的基站被称为接入点（Access Point，AP），它的覆盖范围为几十米；蜂窝电话网的基站被称为蜂窝塔（Cell Tower），在空旷的区域它的覆盖范围为几十千米。只有在基站的覆盖范围内，用户才可能通过它进行数据交互。除此之外，无线网络用户还可以通过自组织的方式形成自组网（Ad-hoc Networks）。它的特点是无须基站和上层网络支持，用户自身具备网络地址指派、路由选择以及类似域名解析等功能。例如：无线传感器网络就是一种典型的自组网。在无线传感器网络中，每个传感器都有一个独一无二的标识符（ID），且每个传感器既是数据的产生者，也是其他节点数据传输的中继。

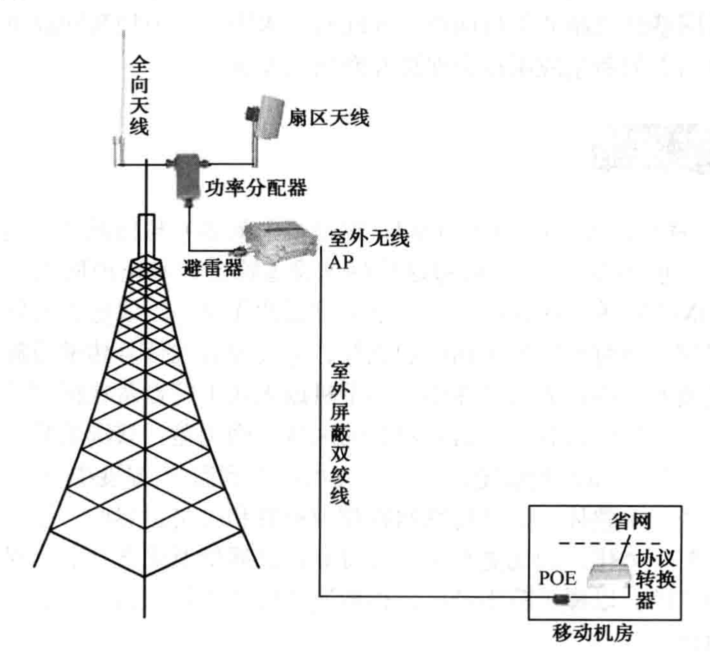


图 4-10　基站

基于采用不同技术和协议的无线连接的传输范围，可以将无线网络分为 4 类，如图 4-11 所示。

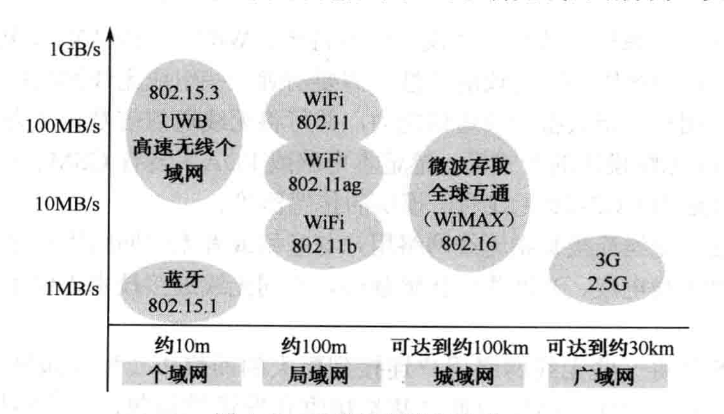


图 4-11　无线网络协议分类



4.2.2 无线网络分类

1. 无线广域网

无线广域网（Wireless Wide Area Networks，WWAN）连接信号可以覆盖整个城市甚至国家，其信号传播途径主要有两种：一种是信号通过多个相邻的地面基站接力传播，另一种是信号可通过通信卫星系统传播。当前主要广域网包括 2G、2.5G 和 3G 系统。2G 系统的核心技术包括全球移动通信系统（Global System for Mobile Communications，GSM）和码分多址数字无线技术（Code Division Multiple Access，CDMA）。

2G 系统的带宽约为 10KB/s；2.5G 系统的带宽为 100～400KB/s，它的核心技术包括通用分组无线业务（General Packet Radio Service，GPRS）和增强型数据速率 GSM 演进技术（Enhanced Data Rates for GSM Evolution，EDGE）；3G 系统的最大带宽约为 2MB/s，核心技术包括 2000 型 CDMA（CDMA-2000）、时分同步码分多址数字无线技术（Time Division Synchronous Code Division Multiple Access，TD-SCDMA）和通用移动通信系统（Universal Mobile Telecommunications System，UMTS）。

2. 无线城域网

无线城域网（Wireless Metropolitan Area Networks，WMAN）基站的信号可以覆盖整个城市区域，在服务区域内的用户可通过基站访问互联网等上层网络。它的主要技术是全球微波互联接入（Worldwide Interoperability for Microwave Access，WiMAX）。

WiMAX 技术近些年越来越受到用户的青睐及网络运营商和硬件制造商的重视。美国的 Clearwire 公司是美国最大的 WiMAX 网络运营商。在我国“无线城市”计划中，WiMAX 是其骨干网络架构的重要组成部分，WiMAX 基站与互联网通过调整回程连接相连，WiMAX 基站与众多 WiFi 接入点相连，这种 WiMAX+WiFi 的方式可为整个城市中的所有无线网络用户提供宽带连接服务。

IEEE 802.16 的一系列协议对 WiMAX 进行了规范。WiMAX 基站的视线（Line of Sight，LoS）覆盖范围可达到 112.6 千米，所谓“LoS”是指无线电波在相对空旷的区域以直线传播，但在建筑相对密集的城市中，无线电波会以非视线（None Line of Sight，NLoS）方式传输，802.16a 协议支持的基站的非视线覆盖范围为 40 千米。WiMAX 基站的传输带宽可达到 75MB/s。图 4-12 是模拟 WiMAX 体系网络架构图。

3. 无线局域网

无线局域网（Wireless Local Area Networks，WLAN）在一个局部的地方（如图书馆、展厅、教学楼、候机大厅、餐厅等）内为用户提供可访问互联网等上层网络的无线连接。

无线局域网有两种工作模式，第一种基于基站（无线局域网内的接入点，AP）模式，无线设备（如 3G 手机、笔记本电脑、iPad、上网本等）通过接入点访问上层网络（见图 4-13）；第二种基于自组织模式，例如在一个会议室内，所有与会者的移动设备都可以不借助接入点组成

一个网络，用于相互之间的文件、视频数据的交换。

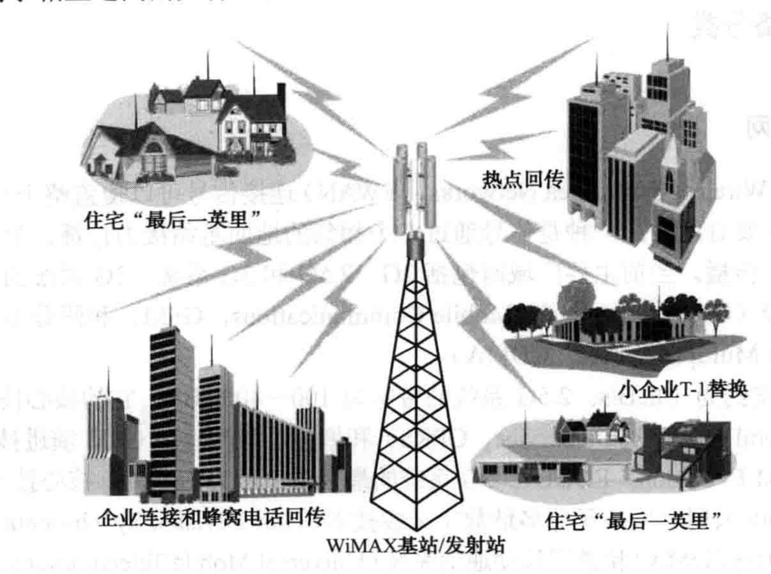


图 4-12　WiMAX 网络架构

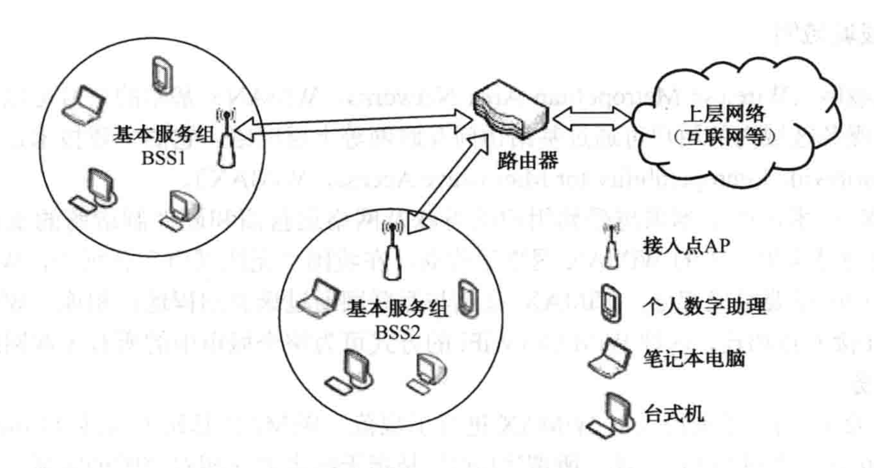


图 4-13　无线局域网 WLAN 架构

IEEE 802.11 的覆盖范围为几十米，802.11b 带宽可达到 11MB/s，802.11a 和 802.11g 的带宽可达到 54MB/s，802.11n 利用多天线多输入多输出（Multiple Input Multiple Output，MIMO）技术，也就是说，在发送端和接收端可能各有两根天线，它们可以同时接收和发送数据包，这样可将 802.11a/g 的带宽提高一倍，可达到 100MB/s 左右，如表 4-1 所示。

表 4-1　802.11 协议对比

802.11 协议	发布时间	频宽（GHz）	最大带宽	调制模式
802.11-1997	1997.06	2.4～2.485	2MB/s	DSSS
802.11a	1999.09	5.1～5.8	54MB/s	OFDM

续表

802.11 协议	发布时间	频宽（GHz）	最大带宽	调制模式
802.11b	1999.09	2.4～2.485	11MB/s	DSSS
802.11g	2003.06	2.4～2.485	54MB/s	DSSS 或 OFDM
802.11n	2009.10	2.4～2.485 或 5.1～5.8	100MB/s	OFDM

4. 无线个人局域网

无线个人局域网（Wireless Personal Area Networks，WPAN）在更小的范围内（约为 10 米）以自组织模式在用户之间建立用于相互通信的无线连接。蓝牙（Bluetooth）传输技术和红外传输技术是无线个人局域网中的两个重要技术。

蓝牙传输技术通过无线电波作为载波，覆盖范围约为 30 米，工作在 2.4GHz 频带，带宽为 1MB/s 左右；红外传输技术使用红外线作为载波，覆盖范围仅为 1 米左右，带宽通常为 100KB/s 左右。

IEEE 802.15 的一系列协议是针对无线个人局域网行为的规范。802.15.1 是蓝牙传输技术协议；802.15.3 是针对超宽带（Ultra Wideband，UWB）个域网物理层和 MAC 层制定的标准，其带宽约为 100MB/s；802.15.4 是针对低带个域网（传感器网络等）物理层和 MAC 层制定的标准。

4.2.3　无线物联世界

WiFi 协议经历了十几年的发展，如今 802.11a/b/g/n 已成为主流的 WiFi 协议（见图 4-14(a)）。IEEE 于 2009 年发布了 802.11n 协议，到 2010 年 6 月，Lenovo、IBM、ASUS、Dell 等品牌的新型号笔记本电脑的主板已经集成了支持 802.11n 的无线网卡，这在一定程度上说明 WiFi 技术已然是连接互联网的重要手段。

而就网络服务运营商而言，WiFi 载波的频率属于免费的公共频段，且每个 WiFi 接入点可为多个网络用户提供宽带服务，如此低成本高效率的互联网接入技术自然会受到广大网络运营商的重视。图 4-14（b）所示为国外街头免费开放的 WiFi 访问点。中国的一些城市（如北京、上海、杭州等）提出要建立“无线城市”的概念（见图 4-15），实践中结合了 WiFi、WiMAX 及 3G 等多种技术，而 WiFi 无疑是“最后一英里”传输的重要组成部分。



（a）



（b）

图 4-14　街道上的 WiFi 接入点及 WiFi 标志



图 4-15　位于上海南京西路的 WiFi 亭

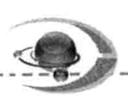
无线宽带网络在网络互联中扮演了越来越重要的角色，相信在不久的将来，地球上只要有人类活动出现的地方都会被无线宽带网络所覆盖，必将为物联网中智能的/非智能的、大的/小的、可移动的/不可移动的无数物体提供更普遍的互联。

4.3　无线低速网络及其协议

物联网的出现使得各种物体之间的无缝连接成为了可能，也标志着更加全面的互联互通成为了可能。可以想象，在物联网中由于各种各样的物体都能够互联起来，随时都能够查询各种物体的状态，小到空调，大到行驶的车辆，甚至还能够对这些物体进行调整、控制。而需要对各种各样的物体进行操作的前提就是首先将它们连接起来，也就是说更全面的互联互通既是物联网的一个重要目标，也是实现物联网其他功能的前提。

物联网更全面的互联互通意味着互联对象从较高智能的计算机和手机，到低智能的一般物体，连接方式也从不断追求更高速向高速与低速相互结合。更加全面的互联互通需要对传统的技术稍加扩展，比如，现在广泛使用的以太网协议不适合直接用来实现全面的互联互通。物联网所连接的已经不仅是传统意义上的主机节点，而是各种各样有智能的、非智能的物体。这些物体不可能每一个都有着同当前互联网设备一样的应用背景，也不可能每一个都有着跟现在互联网设备，如网站服务器、个人计算机、手机、PDA 一样的能力，它们之间也很难像互联网一样通过路由器、交换机等设备有组织地级联起来。因此适用于互联网设备的网络协议并不能完全满足物联网的需求。考虑到各种物体的存在和需求，除了调整的网络协议，相应地还必须要有低速的网络协议。这些网络协议能够适应物联网中那些能力较低的节点的低速率、低通信半径、低计算能力和低能量来源的特征。

低速网络协议非常多，在这里，只介绍当前能够应用于物联网应用的网络通信协议的蓝牙、红外和 802.15.4/ZigBee 协议。



1. 蓝牙

蓝牙，是一种支持设备短距离通信（一般 10 米内）的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换（见图 4-16）。此外蓝牙技术还被大量应用于 GPS 设备、医疗设备，以及游戏平台等各种不同领域。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够成功地简化设备与互联网之间的通信，从而数据传输变得更加迅速高效，为无线通信拓宽道路。蓝牙支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段。其数据速率为 1Mbit/s。采用时分双工传输方案实现全双工传输。



图 4-16　使用蓝牙通信设备

蓝牙这个名称来自于第 10 世纪的一位丹麦国王 Harald Blatand，Blatand 英文意思可解释为 Bluetooth（蓝牙），这是因为国王喜欢吃蓝莓，牙龈每天都是蓝色的缘故。Blatand 国王将现在的挪威、瑞典和丹麦统一起来；他的口齿伶俐，善于交际，因此欧洲人认为用 Blatand 国王的名字命名这项即将面世的技术再合适不过了。

蓝牙的创始人是瑞典 ERICSSON（爱立信）公司，爱立信早在 1994 年就已进行研发。1997 年，爱立信与其他设备生产商联系，并激发了他们对该项技术的浓厚兴趣。1998 年 2 月，5 个跨国大公司，包括 ERICSSON、NOKIA、IBM、TOSHIBA 及 INTEL 组成了一个特殊兴趣小组（Bluetooth Special Interest Group，SIG），他们共同的目标是建立一个全球性的小范围无线通信技术，即现在的蓝牙。

图 4-17 展示了蓝牙标志的由来：它取自 Harald Bluetooth 名字中的「H」和「B」两个字母，用古北欧字母来表示，将这两者结合起来，就成为了蓝牙的 logo。

蓝牙技术联盟（SIG）于 2010 年 4 月 20 日表示，蓝牙 4.0 技术规范已经基本成型，它包括三个子规范，即传统蓝牙技术、高速蓝牙和新的蓝牙低功耗技术。改进之处主要体现在三个方面，电池续航时间、节能和设备种类上。此外，蓝牙 4.0 的有效传输距离也有所提升。当前，蓝牙的有效传输距离为 10 米（约 30 英尺），而蓝牙 4.0 的有效传输距离可达到 60 米（约 200 英尺）。

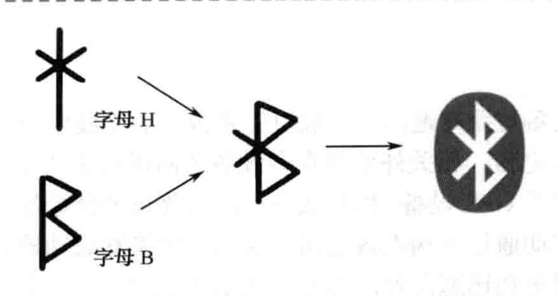


图 4-17　蓝牙标志的来历

在蓝牙通信中，蓝牙设备有两种可能的角色，分别为主设备和从设备。同一个蓝牙设备可以在这两种角色之间转换。一个主蓝牙设备可以最多同时和 7 个从设备通信。在任意时刻，主设备单元可以向从设备单元中的任何一个发送信息，也可以用广播方式实现同时向多个从设备发送信息。

蓝牙作为一种短距离低功耗的传输协议，与传统所使用的 WiFi 协议有什么区别呢？

WiFi 和蓝牙都是 802 系列的无线协议，目的都是取代现在的有线连接。我们常说的 WiFi 其实真正的叫法是 IEEE 802.11b。这两种无线的连接协议都是在 2.4G 的公共频段的，两者都支持跳频。

蓝牙设备之间可以直接通信，WiFi 设备之间要通过 AP 才能通信。因此它们之间的区别就如同对讲机和电话机。

距离：蓝牙一般在 10 米以内，室内距离是 4～5 米。而 WiFi 的距离是 100 米，室内距离是 40～50 米，最远的产品可以达到 96 千米。

技术：蓝牙使用的一般是跳频，而 WiFi 一般是直接序列扩频。

速度：蓝牙低速度，最大速度为 2MB/s，WiFi 高速度，最大速度达 11MB/s。

目的：蓝牙是为不同的电子设备通信而设计的，而 WiFi 是为无线局域网而设计的。

两者之间的侧重点与用途都不同，并不存在相互竞争与冲突，也不能说某一样比另一样更好，只能说两者的存在会形成互补。

2. 红外

红外通信技术（Infrared Communications Technologies）利用 950 纳米近红外波段的红外线作为传递信息的媒体，即通信信道，通信距离一般为 1 米左右。其出现早于蓝牙通信技术，是一种比较早的无线通信技术。由红外数据协会（Infrared Data Association，IrDA）来建立统一的红外通信标准。其发送端将基带二进制信号调制为一系列的脉冲串信号，通过红外发射管发射红外信号。接收端将接收到的光脉转换成电信号，再经过放大、滤波等处理后送给解调电路进行解调，还原为二进制数字信号后输出。常用的有通过脉冲宽度来实现信号调制的脉宽调制（PWM）和通过脉冲串之间的时间间隔来实现信号调制的脉时调制（PPM）两种方法。

红外通信有保密性强、信息容量大、结构简单（可在室内使用，也可在野外使用）、设备



体积小、成本低、功耗低、不需要频率申请等优点。但由于红外通信使用的波长较短，对障碍物的衍射较差，因此两个使用红外通信的设备之间必须互相可视。另外红外射束易受尘埃、雨水等物质的吸收，影响通信质量。

红外通信技术在 20 世纪 90 年代比较流行，后来就慢慢地被蓝牙和 WiFi 所取代了。主要原因由于设备之间必须可见，通信距离相对蓝牙和其他协议也更加有限。此外，红外设备在通信过程中不能移动使得该技术很难用于外部设备，如鼠标、耳机上，而这些应用使用同属于短距离通信的蓝牙协议则特别合适。尽管如此，目前仍然有很多设备，如手机、笔记本电脑，保留了对红外协议的兼容性。图 4-18 显示了一些典型的红外设备。



图 4-18　典型红外设备

表 4-2 给出红外、蓝牙和高速 WiFi 三种协议的简单对比。在互联网应用中，使用较多的是 WiFi 协议，可以看出虽然调整网络 WiFi 协议有着更高的带宽，但是由于其更远的通信距离和更高的速率，耗电量也相应提高。不难看出，WiFi 协议是为了替代传统的网络中的有线设置，为了适用于互联网的各种应用，在 WiFi 协议的设计过程中，能量考虑不是主要因素。物联网设计中，不是每一个被连接的物体都有着稳定的能量供应，不是每个物体都有强大的计算能力，也不是每个物体都有跟传统互联网一样的应用需求，因此协议设计的方面引用了新的要求，这些要求在传统的互联网应用中没有存在或者并没有那么明显。关键的是需要设计低功耗和复杂度低的通信协议。这些协议会在一定程度上牺牲节点的通信半径或者速率，甚至节点通信的稳定性和安全性。在物联网的通信协议设计中，考虑的问题将是多方面的。在多样化的设备上，如何设计一个良好的通信协议使其能够适应各种应用环境是人们面临的一个挑战。

表 4-2　红外、蓝牙和 WiFi 三种协议简单对比

协议类型	频　段	距　离	耗　电	速　率
红外	3.4kGHz（波长 900 纳米左右）	1 米左右	较低	几十 KB/s 到 1GB/s
蓝牙	2.402GHz～2.480GHz	几米至几百米	较低	1MB/s 到几十兆速率
WiFi	2.4GHz/3.6GHz/5GHz	百米量级	高	大于百兆量级

3. 802.15.4/ZigBee

无线传感网作为物联网的一个典型应用，在其上开发出了一系列通信协议。这些协议考虑了传感器的低功耗、低复杂度的需求，对物联网通信协议的设计也起到了很大的借鉴作用。其

中，802.15.4/ZigBee 协议是最早出现在无线传感网领域的无线通信协议，它介于无线标记技术与蓝牙之间的技术，此前被称作 Home RF Lite 或 FireFly 无线技术，主要用于近距离无线连接，通过数千个微小的传感器之间相互协调来实现通信。这些传感器只需要很少的能量，以接力的方式，通过无线电波将数据从一个传感器传送到另一个传感器，所以通信效率非常高。而这些数据就可以进入计算机用于分析，或者被 WiMAX 收集。

4.4 实训

4.4.1 实训一：无线通信路由配置

1. 任务目标

（1）按照指定的拓扑结构图在 CISCO 模拟器上搭建网络环境。
（2）根据指定的接口、IP 地址等配置路由器和主机。
（3）测试、调试网络通信，使所有计算机能顺利通信。

2. 设备准备

CISCO 模拟器。

3. 任务实施

步骤 1：在 CISCO 模拟器上，按图 4-19 所示网络架构搭建网络环境。笔记本电脑采用无线方式与 R2 进行连接，并在 R2 上开启 DHCP 功能为笔记本电脑分配 IP 参数。

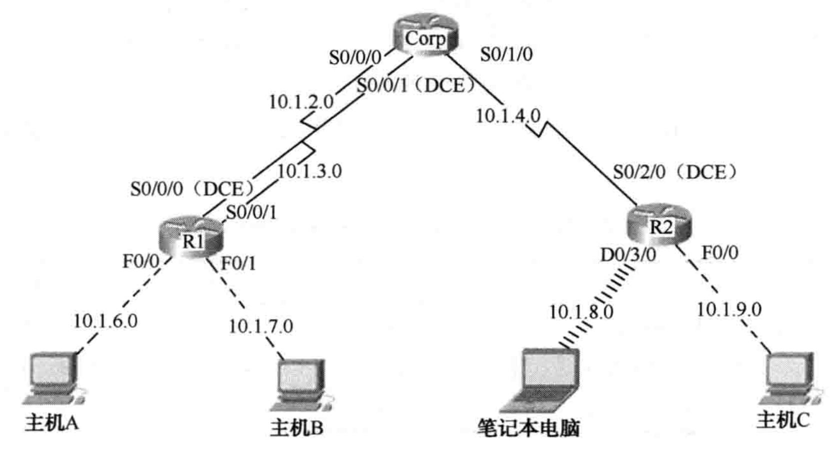


图 4-19　模拟无线通信网络拓扑结构图

步骤 2：在所有路由器上按表 4-3 指定的 IP 地址配置路由。



表 4-3 路由器 IP 地址参数

设备名称	接　口	网络地址	IP 地址
路由器 Corp			
Corp	S0/0/0	10.1.2.0/24	10.1.2.1/24
Corp	S0/0/1（DCE）	10.1.3.0/24	10.1.3.1/24
Corp	S0/1/0	10.1.4.0/24	10.1.4.1/24
路由器 R1			
R1	S0/0/0（DCE）	10.1.2.0/24	10.1.2.2/24
R1	S0/0/1	10.1.3.0/24	10.1.3.2/24
R1	F0/0	10.1.6.0/24	10.1.6.1/24
R1	F0/1	10.1.7.0/24	10.1.7.1/24
路由器 R2			
R2	S0/2/0（DCE）	10.1.4.0/24	10.1.4.2/24
R2	D0/3/0	10.1.8.0/24	10.1.8.1/24
R2	F0/0	10.1.9.0/24	10.1.9.1/24

具体操作如下：

（1）路由器 Corp 的配置。

① 修改路由器的主机名称：

```
Router> enable
Router# configure terminal
Router(config)# hostname Corp
Corp(config)#
```

② 配置路由器 S0/0/0 端口：

```
Corp(config)# interface S0/0/0
Corp(config-if)# ip address 10.1.2.1   255.255.255.0
Corp(config-if)# no shutdown
```

③ 配置路由器 S0/0/1 端口：

```
Corp(config)# interface S0/0/1
Corp(config-if)# ip address 10.1.3.1   255.255.255.0
Corp(config-if)# clock rate 128000
Corp(config-if)# no shutdown
```

④ 配置路由器 S0/1/0 端口：

```
Corp(config)# interface S0/1/0
Corp(config-if)# ip address 10.1.4.1   255.255.255.0
Corp(config-if)# no shutdown
```

⑤ 配置路由器的 RIP 路由：

```
Corp(config)# router rip
Corp(config-router)# version 2
Corp(config-router)# network 10.0.0.0
```

（2）路由器 R1 的配置。

① 修改路由器的主机名称：

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

② 配置路由器 S0/0/0 端口：

```
R1(config)# interface S0/0/0
R1(config-if)# ip address 10.1.2.2    255.255.255.0
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
```

③ 配置路由器 S0/0/1 端口：

```
R1(config)# interface S0/0/1
R1 (config-if)# ip address 10.1.3.2    255.255.255.0
R1 (config-if)# no shutdown
```

④ 配置路由器 F0/0 端口：

```
R1(config)# interface F0/0
R1(config-if)# ip address 10.1.6.1    255.255.255.0
R1(config-if)# no shutdown
```

⑤ 配置路由器 F0/1 端口：

```
R1(config)# interface F0/1
R1(config-if)# ip address 10.1.7.1    255.255.255.0
R1(config-if)# no shutdown
```

⑥ 配置路由器的 RIP 路由：

```
R1(config)# router rip
R1 (config-router)# version 2
R1(config-router)# network 10.0.0.0
```

（3）路由器 R2 的配置。

① 修改路由器的主机名称：

```
Router> enable
Router# configure terminal
Router(config)# hostname R2
R2(config)#
```



② 配置路由器 S0/2/0 端口：

```
R2(config)# interface S0/2/0
R2(config-if)# ip address 10.1.4.2   255.255.255.0
R2(config-if)# clock rate 128000
R2(config-if)# no shutdown
```

③ 配置路由器 F0/0 端口：

```
R2(config)# interface F0/0
R2(config-if)# ip address 10.1.9.1   255.255.255.0
R2(config-if)# no shutdown
```

④ 配置路由器 D0/3/0 端口（无线）：

```
R2(config)# interface D0/3/0
R2(config-if)# ip address 10.1.8.1   255.255.255.0
R2(config-if)# ssid ADMIN
R2(config-if)# no shutdown
```

⑤ 配置路由器的 DHCP 服务器：

```
R2(config)# ip dhcp pool Admin
R2(dhcp-config)# network 10.1.8.0   255.255.255.0
R2(dhcp-config)# default-router 10.1.8.1
R2(dhcp-config)# exit
R2(config)# ip dhcp excluded-address 10.1.8.1
```

⑥ 配置路由器的 RIP 路由：

```
R2(config)# router rip
R2 (config-router)# version 2
R2 (config-router)# network 10.0.0.0
```

步骤 3：在所有计算机上按表 4-4 指定的 IP 地址配置。

表 4-4　计算机 IP 地址参数

设备名称	IP 地址	子网掩码	默认网关
主机 A	10.1.6.2	255.255.255.0	10.1.6.1
主机 B	10.1.7.2	255.255.255.0	10.1.7.1
主机 C	10.1.9.2	255.255.255.0	10.1.9.1
笔记本电脑	使用 DHCP 分配		

步骤 4：测试。在主机 A 上利用 Ping 命令测试：

- Ping　10.1.7.2
- Ping　10.1.8.2
- Ping　10.1.9.2

4.4.2 实训二：建立 WiFi 无线宽带网络

1. 任务目标

本实训通过 WiFi 技术构建局部网络，即开启 Windows 7 的隐藏功能：虚拟 WiFi 和 SoftAP（即虚拟无线 AP），让 PC 变成无线路由器，实现共享上网功能，节省上网费和路由器购置费。

2. 设备准备

带 Windows 7 系统和蓝牙功能的笔记本电脑一台。

3. 任务实施

步骤 1：在“开始”→“运行”命令行中输入“C:\...\cmd.exe”，以管理员身份运行。

步骤 2：启用并设定虚拟 WiFi 网卡。通过运行“netsh wlan set hostednetwork mode=allow ssid=STIEI key=12345678”启用并设定无线网络连接 2，如图 4-20 所示。

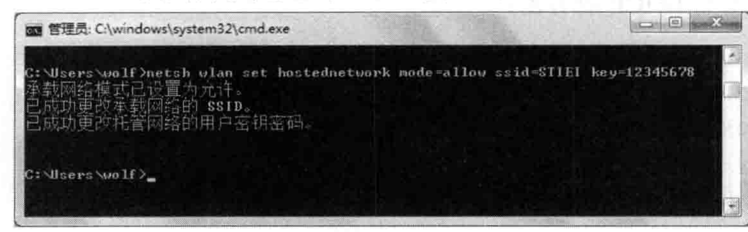


图 4-20　启用并设定无线网络连接 2

此命令有三个参数：

（1）mode：是否启用虚拟 WiFi 网卡，“allow”值为启用，“disallow”为禁用。

（2）ssid：无线网名称，在此以 STIEI 为例。

（3）key：无线网密码，八个以上字符（以 12345678 为例）。

以上三个参数可以单独使用，例如只使用 mode=disallow 可以直接禁用虚拟 WiFi 网卡。

开启成功后，网络连接中会多出一个网卡为“Microsoft Virtual WiFi Miniport Adapter”的无线网络连接 2，这可从“控制面板”→“网络和 Internet”→“网络和共享中心”中选择“更改适配器设置”命令，后打开图 4-21 所示的界面。为方便起见，可右击“无线网络连接 2”，通过“重命名”将其更名为“虚拟 WiFi”，如图 4-21 所示。



图 4-21　新建无线网络连接 2



步骤3：设置Internet连接共享。在图4-22“网络连接”窗口中，右击已连接到Internet的网络连接（如选择“移动宽带连接2”），选择“属性”→“共享”命令，勾选“允许其他网络用户通过此计算机的Internet连接来连接（N）”选项并选择“虚拟WiFi”（见图4-23）。确定之后，提供共享的网卡图标旁会出现“共享的”字样，表示“移动宽带连接2”已共享至“虚拟WiFi”，如图4-24所示。

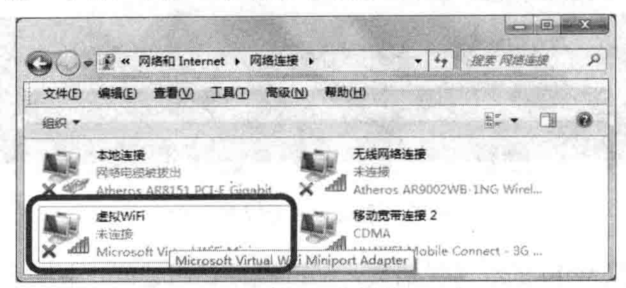


图4-22 更名为“虚拟WiFi”

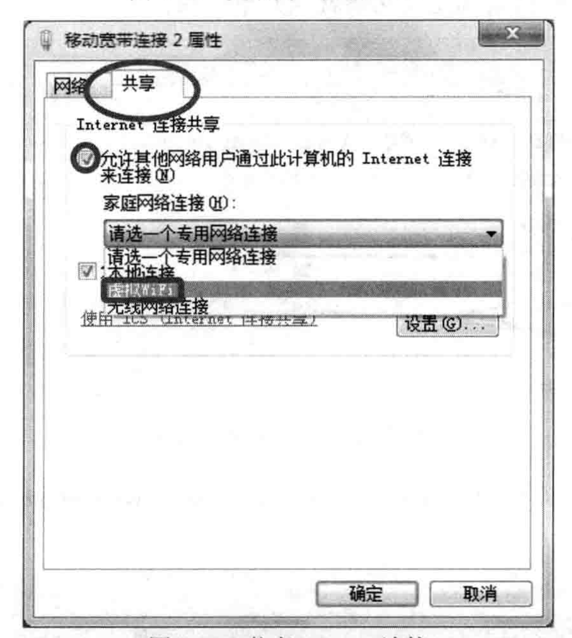


图4-23 共享Internet连接

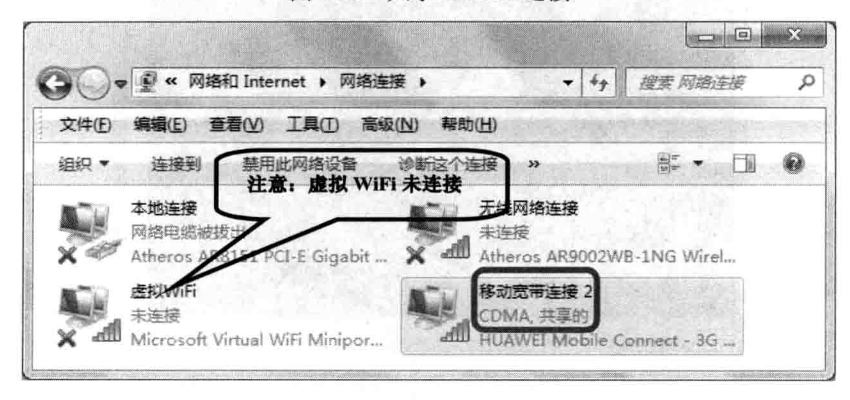


图4-24 无线CDMA共享上网

步骤4：开启无线网络。只需在图4-25所示命令行提示符中运行“netsh wlan start hostednetwork”即可（注：若参数start改为stop即可关闭该无线网，开机后要启用该无线网只需再次运行此命令）。

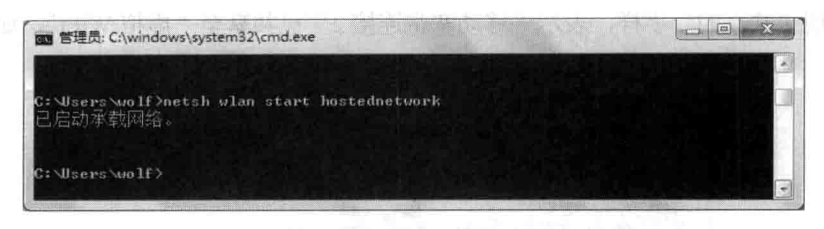


图4-25　输入开启无线网络命令

至此，图4-26虚拟WiFi的红叉叉消失，WiFi基站已组建好，主机设置完毕。笔记本电脑、带WiFi模块的手机等子机搜索到无线网络就能共享上网。

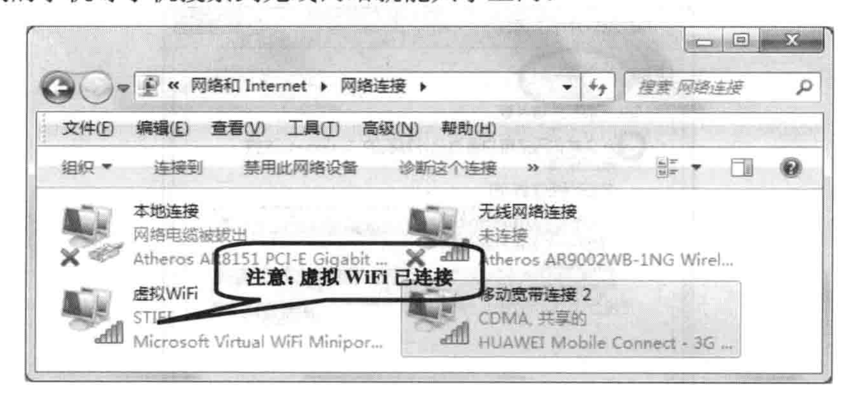


图4-26　虚拟WiFi已连接

步骤5：显示无线网络信息。在命令行中输入“netsh wlan show hostednetwork”，显示图4-27所示的结果。



图4-27　无线网络信息



虚拟无线 AP 发射的 WLAN 是 802.11n 标准，带宽为 100Mbit/s。

步骤 6：更改 WPA2-PSK 密码。图 4-27 显示密码为 CCMP。若改为“STIEI”，在命令行中输入“netsh wlan refresh hostednetwork STIEI”。

更改密码后必须再次手动启用虚拟网络。

步骤 7：关闭虚拟网络。输入“netsh wlan stop hostednetwork”即可，如图 4-28 所示。

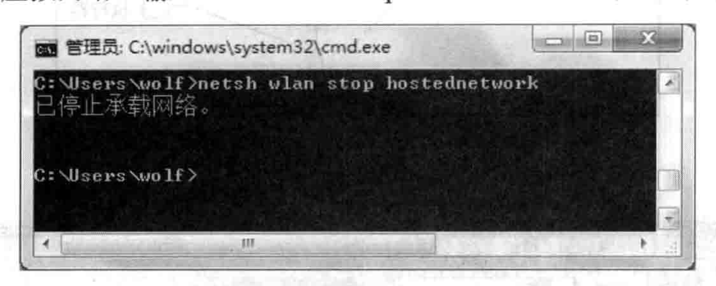


图 4-28 关闭虚拟 WiFi

4.4.3 实训三：蓝牙无线传感数据采集与控制

1. 任务目标

（1）对蓝牙模块进行设置，与蓝牙适配器进行配对，组建蓝牙无线网络。

（2）了解蓝牙无线传感数据采集。

（3）了解蓝牙无线传感数据控制。

2. 设备准备

（1）蓝牙无线传感控制节点。

（2）蓝牙适配器。

（3）操作台：提供电源、PC、USB 口、RS232 串口。

（4）软件：上位机软件。

3. 任务实施

构建蓝牙无线网络环境。利用下面传感控制节点蓝牙配置命令，设置蓝牙从节点的设备名称和配对密码，然后在监控服务器上利用蓝牙主节点，发现各个蓝牙从节点，从而组建图 4-29 所示的蓝牙网络结构，并利用监控服务器上的软件对蓝牙传感控制节点进行传感数据采集和控制。

步骤 1：将蓝牙传感控制节点与 PC 串口相连。

步骤 2：设置蓝牙传感控制节点上的蓝牙模块。打开 AccessPort 串口工具，进行参数配置，如图 4-30 所示。

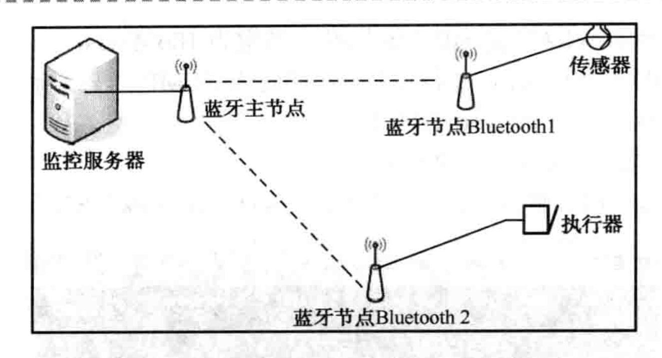


图 4-29　蓝牙无线网络结构

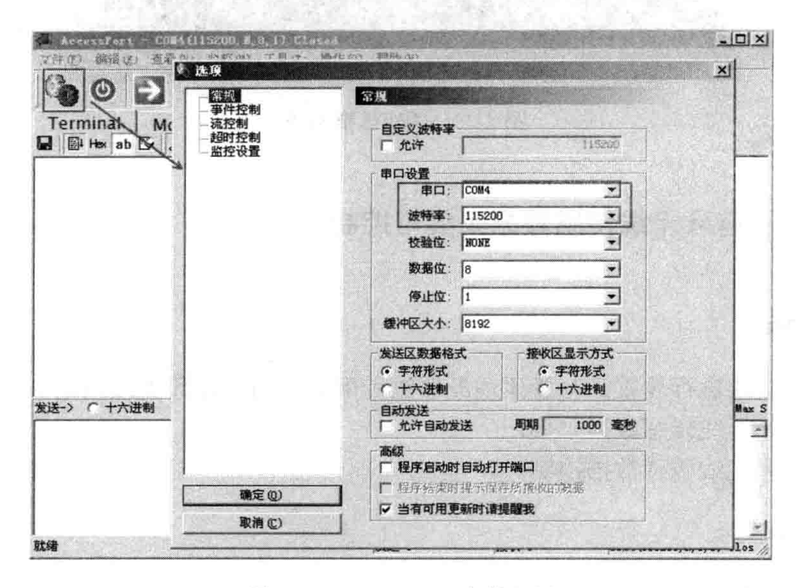


图 4-30　AccessPort 参数配置

步骤 3：设置配对密码和设备名称。

（1）设置 AT+PIN，蓝牙配对密码。AT+PIN 后紧接 4 位配对密码，限数字，字符无效，如图 4-31 所示。

例：AT+PIN1234

返回<CR><LF>AT+PIN1234[空格]OK<CR><LF> 配置正确

<CR><LF>AT+PIN1234[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

（2）设置 AT+NAME，设置设备名称。AT+NAME 后面紧接 20 位以内的数字或字符，如图 4-32 所示。

例：AT+NAMEBuletooh1

返回<CR><LF>AT+NAMEBuletooh1[空格]OK<CR><LF> 配置正确

<CR><LF>AT+NAMEBuletooh1[空格]ERROR<CR><LF>配置错误

<CR><LF>ERROR<CR><LF>命令错误



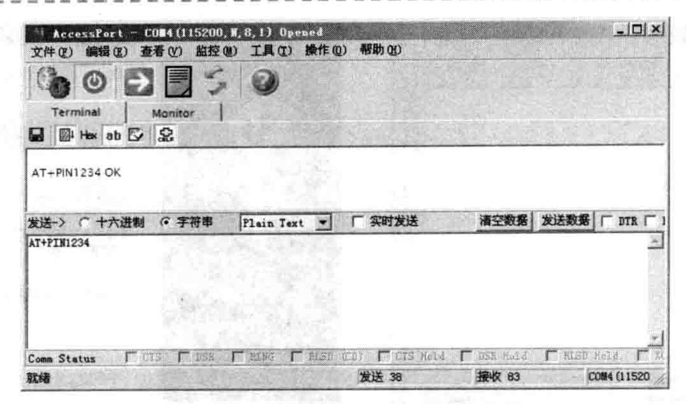


图 4-31　配置配对密码

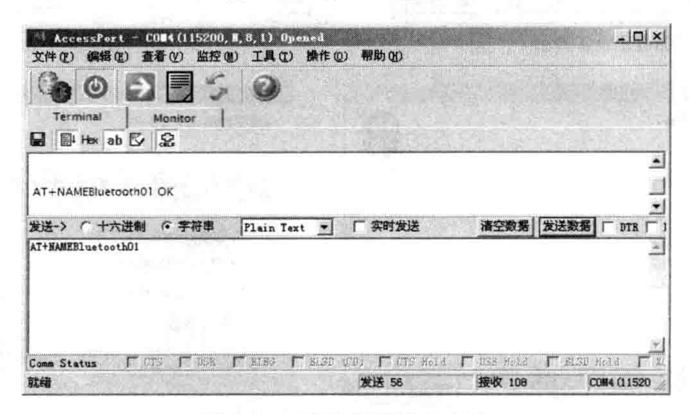


图 4-32　设置蓝牙设备名称

（3）查询 AT+VERSION 蓝牙版本号。输入命令“AT+VERSION”即可。

步骤 4：重启模块。在图 4-33 中输入命令“AT+RESET OK”重启模块保存设置。

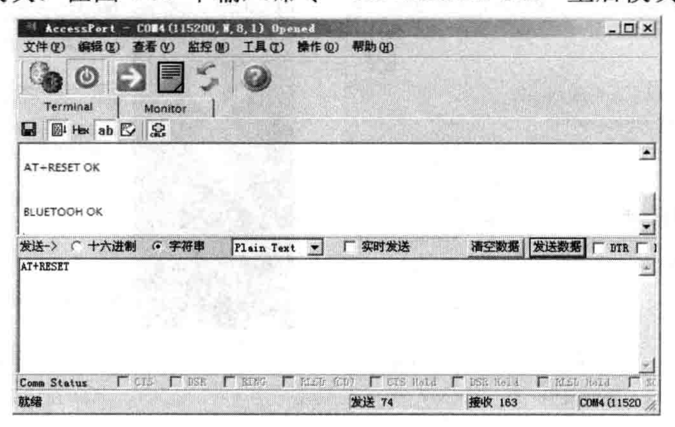
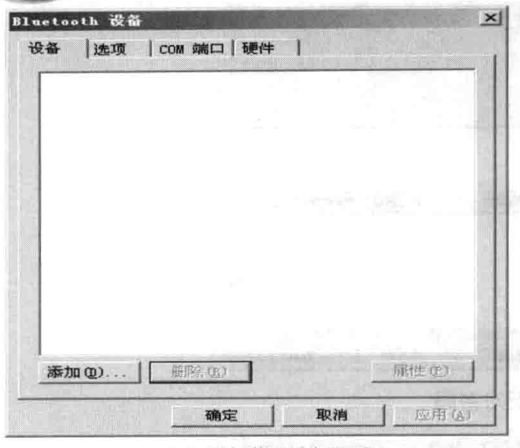
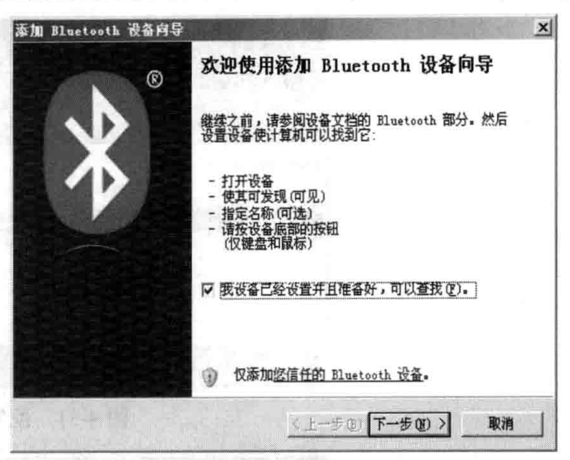


图 4-33　重启模块

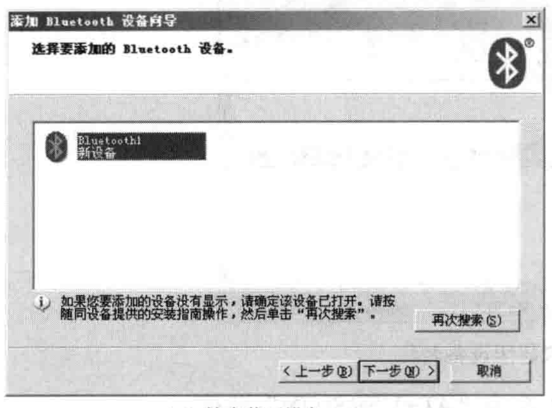
步骤 5：生成虚拟串口。在蓝牙主节点 PC 上添加蓝牙从节点设备（即蓝牙传感控制节点），生成虚拟串口（传入和传出），如图 4-34 所示。



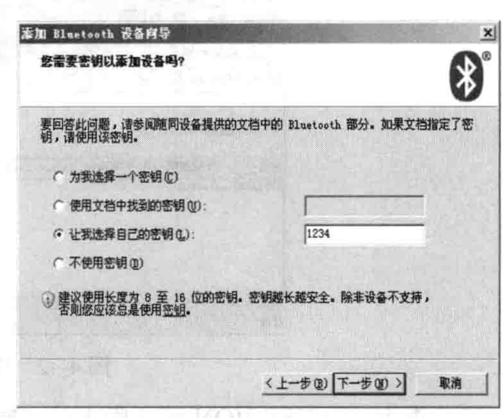
（a）添加蓝牙设备界面



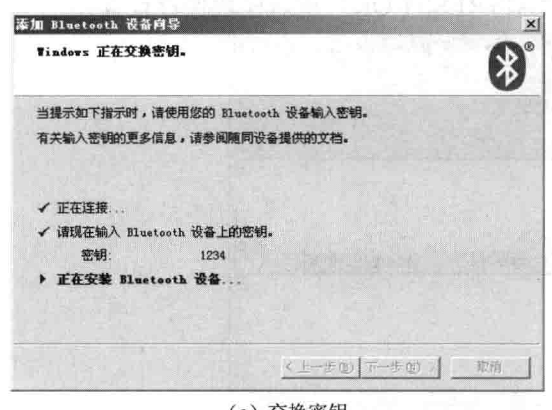
（b）添加设备向导



（c）搜索蓝牙设备



（d）选择设备密码



（e）交换密钥



（f）生成虚拟串口

图 4-34　添加蓝牙设备生成虚拟串口

步骤 6：查看蓝牙设备虚拟 COM 口，如图 4-35 所示。



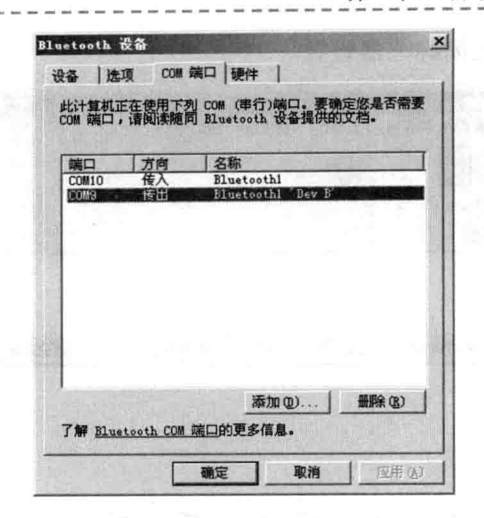


图 4-35　查看添加蓝牙设备生成的虚拟串口

至此，蓝牙无线网络已组建成功，后面的实验就可以采用生成的虚拟串口来完成蓝牙数据采集和控制。

步骤 7：蓝牙无线数据采集与控制。在蓝牙主机上打开监控软件 AccessPort，通过上面生成的虚拟串口 COM9 远程采集传感数据与控制，如图 4-36 所示。

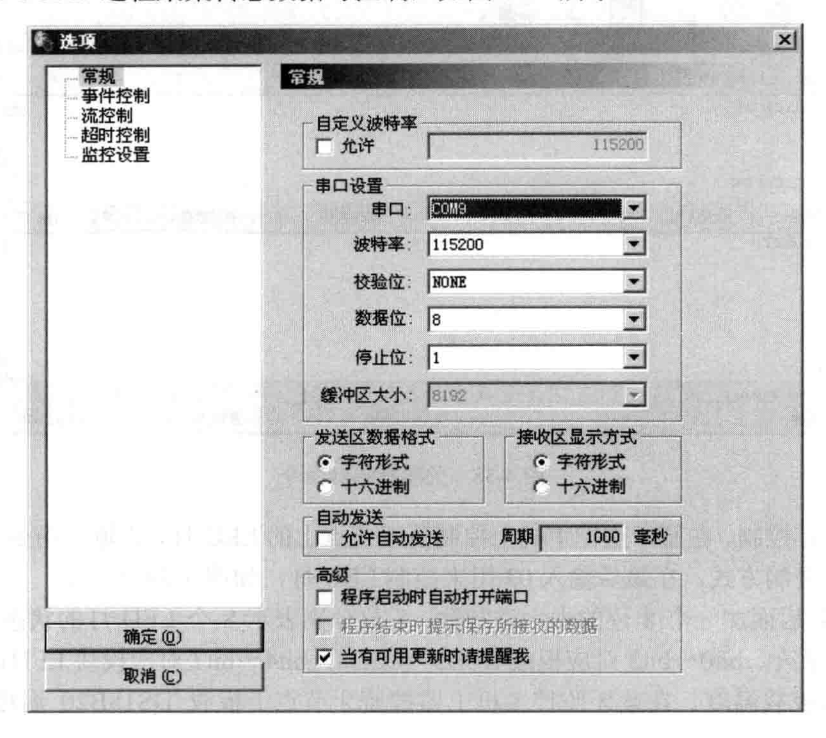


图 4-36　设置虚拟串口参数

（1）蜂鸣器控制。在蓝牙监控主机上控制蓝牙节点上的蜂鸣器，如图 4-37 所示打开蜂

鸣器设置，如图 4-38 所示关闭蜂鸣器设置。

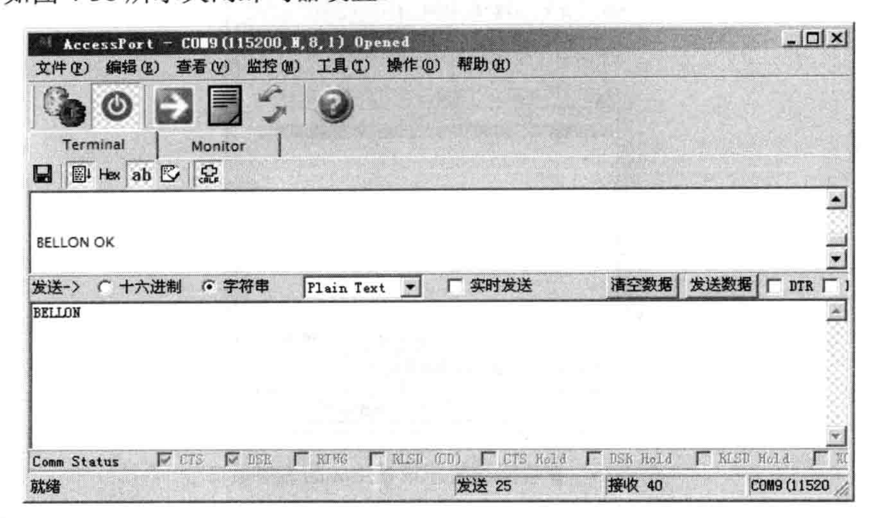


图 4-37　打开蜂鸣器命令

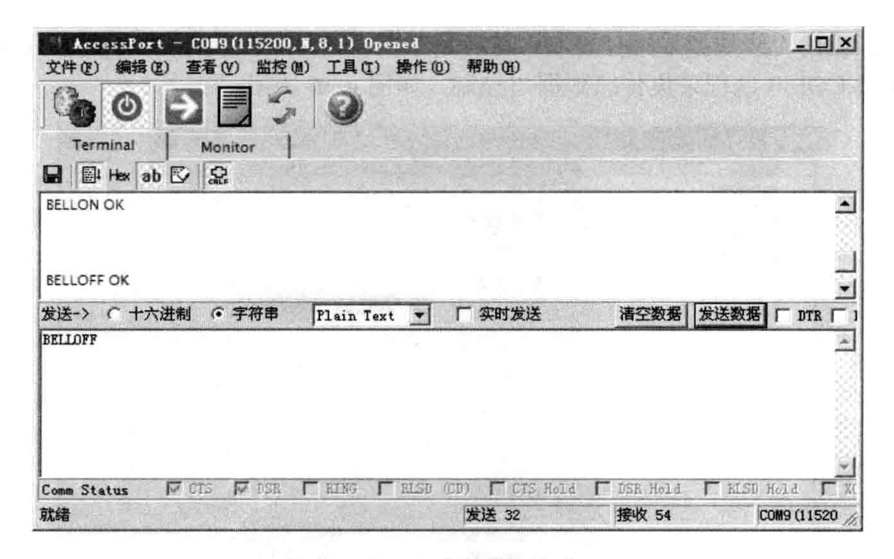


图 4-38　关闭蜂鸣器命令

（2）LED 灯控制。在蓝牙监控主机上控制蓝牙节点上的 LED 灯，先输入指令“LED1SET”，然后选择十六进制方式，在最后输入 03 用来控制 LED 灯，如图 4-39 所示。

LED1SET 后面加一个 8 位的十六进制数，8 位分别表示 8 个 LED 灯的状态，对应位为 0 表示亮，1 表示灭。bit0～bit3 对应板载 LED5～LED8，bit4～bit7 对应模块 LED1～LED4。

（3）采集板载温度。在蓝牙监控主机上监控蓝牙节点上板载 DS18B20 温度，如图 4-40 所示。



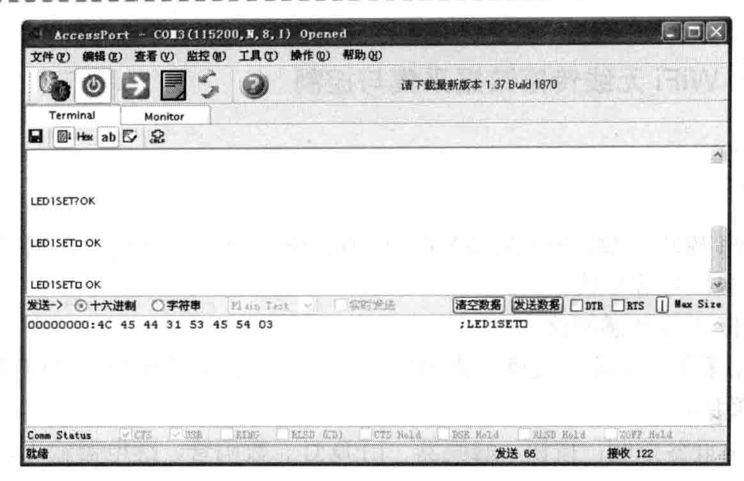


图 4-39　控制 LED 灯

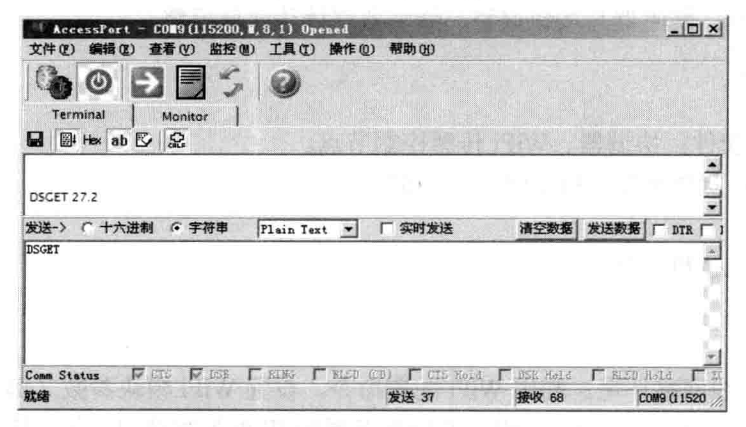


图 4-40　采集蓝牙节点板载温度

（4）采集板载光照度。在蓝牙监控主机上监控蓝牙节点上板载光照度，如图 4-41 所示。

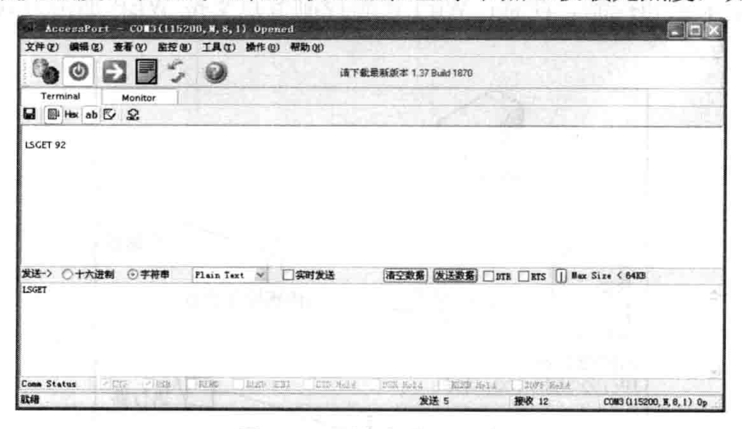


图 4-41　采集板载光照度

其他采集数据和控制命令详情见附录二。

4.4.4 实训四：WiFi 无线传感数据采集与控制

1. 任务目标

（1）设置 WiFi 模块参数：SSID、KEY、信道、IP 地址、子网掩码、网关、DNS、监控服务器的 IP 地址和端口号等参数。

（2）组建 WiFi 无线传感网络。

（3）传感数据采集：温度、湿度、光照度、人体感应、烟雾探测、可燃气体探测、三轴加速度传感器数据采集。

（4）输入/输出设备控制：按钮、蜂鸣器、LED 灯、数码管、继电器输出、直流电机、步进电机。

（5）关联控制：蜂鸣器与按钮报警、蜂鸣器气体传感器报警。

2. 设备准备

（1）ZigBee 套件：协调器、WiFi 传感控制节点。

（2）操作台：提供电源、PC、串口、USB 口。

（3）服务器。

（4）软件：上位机软件。

3. 任务实施

构建 WiFi 无线网络环境。利用 WiFi 配置命令，设置 WiFi 模块参数（例如 SSID、KEY、信道、IP 地址、子网掩码、网关、DNS、监控服务器的 IP 地址和端口号等，其中，SSID 和 KEY 与无线路由器一致），构建结构如图 4-42 所示。然后利用监控服务器上的软件对 WiFi 传感控制节点进行传感数据采集和控制。注意：WiFi 传感控制节点支持 WEP 加密方式，因此无线路由设置为 WEP 加密方式。

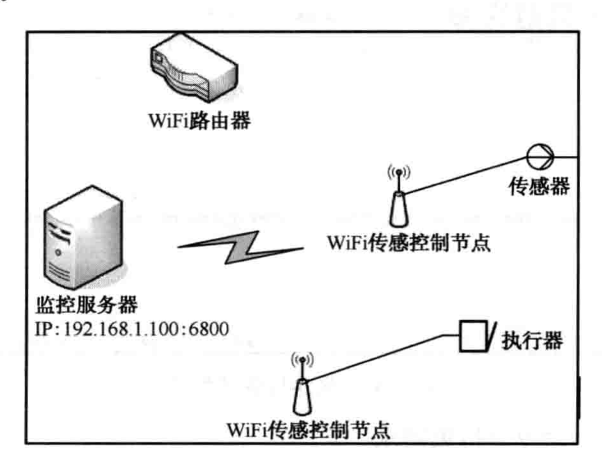
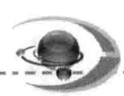


图 4-42　WiFi 网络结构



步骤 1：WiFi 无线模块设置。取 WiFi 控制模块（CH-RB801 板），将“WiFi 参数设置跳线端口”上的两个跳线帽从“RUN”处拔出，接到下方“RESET”两个端口处（注意：正常通信时，必须要将跳线帽恢复到“RUN”处）。

将 WiFi 模块插入相应接口、拔掉其他在板模块（包括 LCD 模块）。

步骤 2：设置无线路由器。以图 4-43 所示 TP-Link 无线路由器为例，在 IE 浏览器 URL 中输入“http://192.168.1.1”，登录用户名和密码为 admin，打开无线路由器 Web 页面，即可进行无线设置和无线安全设置，主要设置 SSID、信道、加密方式与密钥等。注意，WiFi 的 SSID、信道、加密方式与密钥等要和无线路由一样。

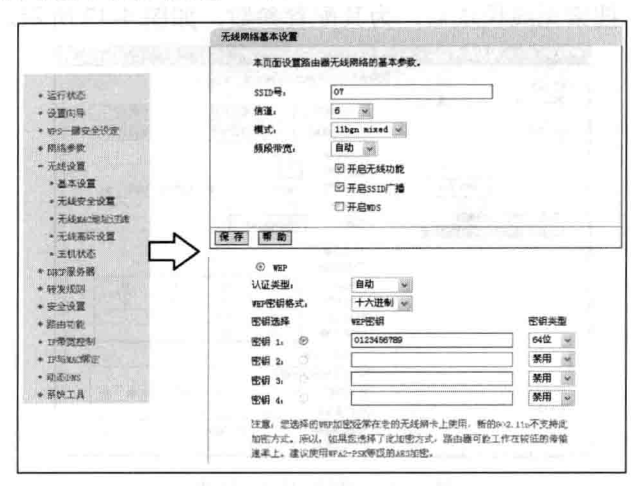


图 4-43　无线路由设置

步骤 3：设置串口退出“透传模式”及配置参数。连接串口，通电，在上位机上打开 UART-WiFi UART 配置管理程序，进行 WiFi 参数设置。

WiFi 无线通信模块默认出厂波特率为 115200，选择相对应串口，单击“设置”按钮，如图 4-44 所示。

图 4-44　UART-WiFi 串口参数设置

选择“确定”、“退出”后，退出“透传模式”，如图 4-45 所示。如果出现了图 4-46 所示的提示，则要检查模块是否已通电、COM1 口是否已经打开以及波特率是否设置正确。

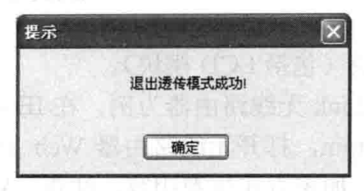


图 4-45　退出透传模式成功

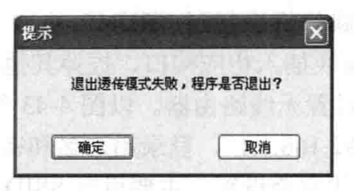


图 4-46　退出透传模式失败

单击[搜索模块]按钮，搜索无线模块后，为其配置参数，如图 4-47 所示。



图 4-47　配置 WiFi 参数

单击[提交修改]按钮后，WiFi 模块就设置完成。然后再将 WiFi 模块取下接到图 4-48 所示的板子上。

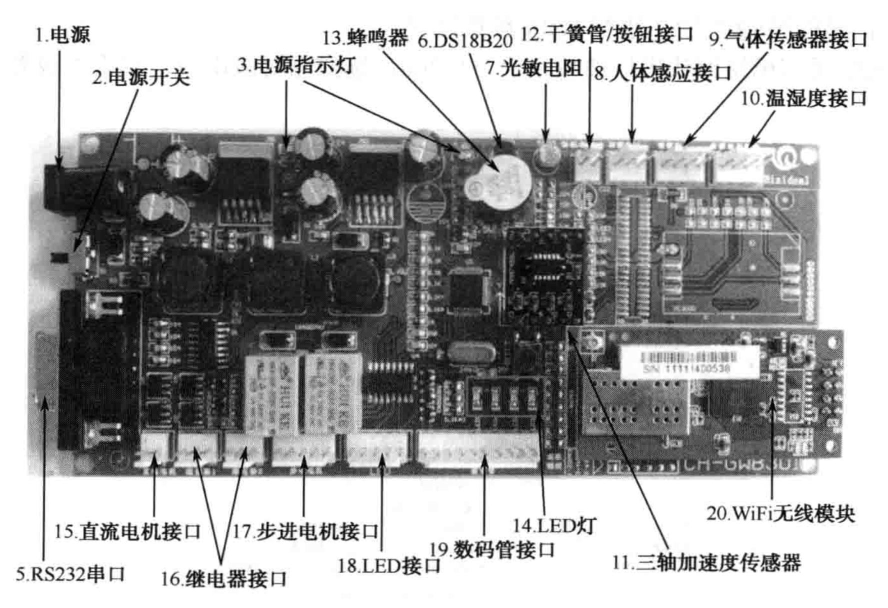


图 4-48　WiFi 传感控制节点



步骤 4：打开监听软件，查看 WiFi 无线网络组建情况。双击TCP&UDPDebug图标，打开监听软件。单击"创建服务器"按钮，如图 4-49 和图 4-50 所示。注意，TCP 端口要和 WiFi 模块设置的端口号一致，否则，WiFi 模块无法成功连接到无线路由器上。



图 4-49　TCP&UDP 测试工具

创建服务器

指定IP 192.168.1.2

本机端口： 60000

每隔 30 秒自动断开与客户端的连接

确定　取消

图 4-50　TCP 端口设置

单击"启动服务器"按钮将监控服务器上的监控软件打开，软件开始监听端口，如图 4-51 所示。

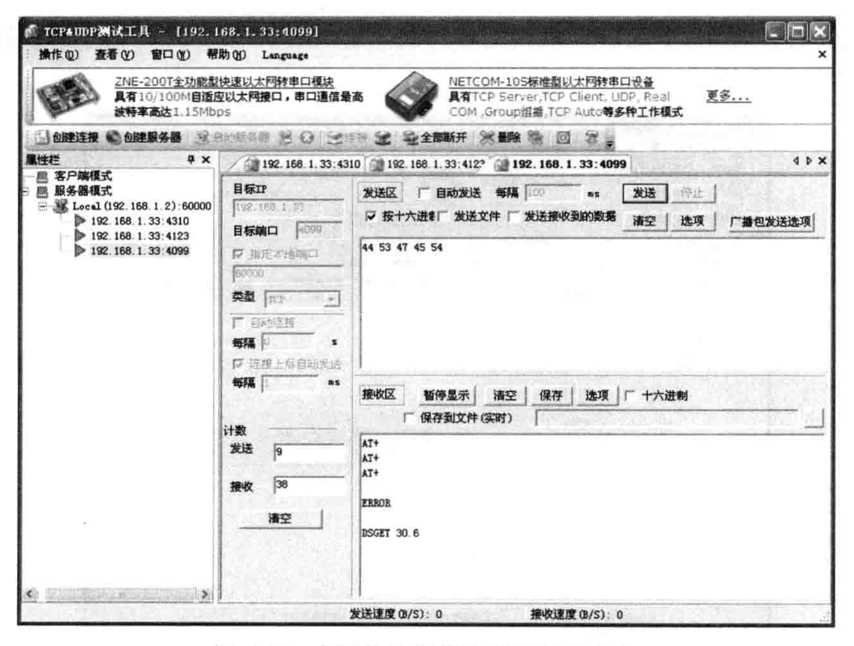


图 4-51　在服务器端查看 WiFi 连接状态

至此，WiFi 无线网络已组建成功。注意：由于监听软件是间隔的和 WiFi 模块通信，所以过了一定时间间隔就会出现新的客户端，选择新的客户端再发送数据。

接下来，仅举几个 WiFi 无线控制与传感数据采集的例子，其余请参考附录二。

步骤 5：控制蜂鸣器。在监控服务器上选择所连接的客户端，在数据发送区输入“BELLON”指令，手动发送，此时 WiFi 节点上的蜂鸣器开始报警；然后再发送停止报警指令“BELLOFF”，此时 WiFi 节点上的蜂鸣器停止报警，如图 4-52 所示。

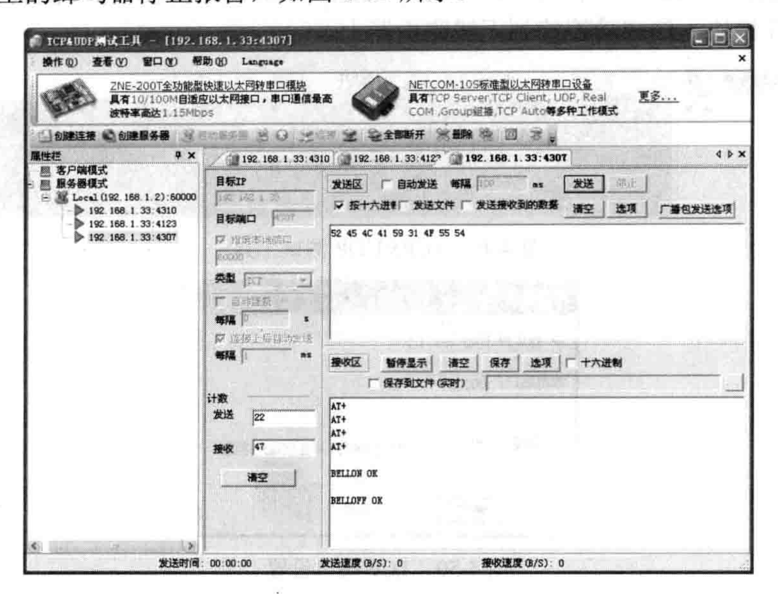


图 4-52　发送蜂鸣器报警与停止指令

步骤 6：采集板载温度。选择所连接的客户端，输入指令“DSGET”，手动发送，返回当前板载温度，如图 4-53 所示。



图 4-53　采集板载温度

注意：发送区数据可以是十六进制的，也可以是 AT 指令，如果用 AT 指令必须把“按十六进制”前面的钩去掉。AT 指令必须是大写的，如图 4-53 所示。



4.4.5　实训五：GPRS 无线传感数据采集与控制

1. 任务目标

（1）设置 GPRS 模块参数：启用/禁用 GSM 网络和 GPRS 网络功能，指定 Internet 上监控服务器的 IP 地址和端口号。

（2）组建 GPRS 无线网络。

（3）传感数据采集：温度、湿度、光照度、人体感应、烟雾探测、可燃气体探测、三轴加速度传感器数据采集。

（4）输入/输出设备控制：按钮、蜂鸣器、LED 灯、数码管、继电器输出、直流电机、步进电机。

（5）关联控制：蜂鸣器与按钮报警、蜂鸣器气体传感器报警。

2. 设备准备

（1）ZigBee 套件：协调器、GPRS 无线传感控制节点。

（2）操作台：提供电源、PC、USB 口、RS232 串口。

（3）SIM 卡。

（4）软件：上位机软件。

3. 任务实施

步骤 1：构建图 4-54 所示的 WiFi 无线网络环境。利用 AccessPort 通过串口对传感控制节点上的 GPRS 模块进行设置。

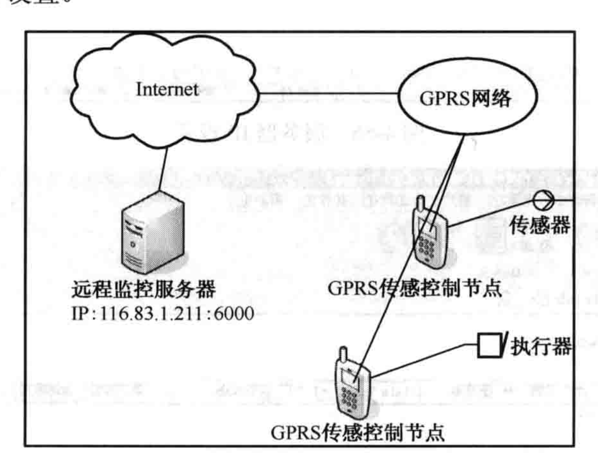


图 4-54　GPRS 无线网络架构

（1）打开 Internet 远程监控服务器端口。注意，192.168.1.7 为局域网内一台机器，已在路由器上为其设置了 NAT 映射，其对外网的 IP 地址为 116.83.1.211，并打开了 TCP 6000 端口，

如图 4-55 所示。

图 4-55　打开服务器监听端口

（2）设置 GPRS 模块，指定 Internet 远程监控服务器 IP 地址和端口，如图 4-56 和图 4-57 所示。

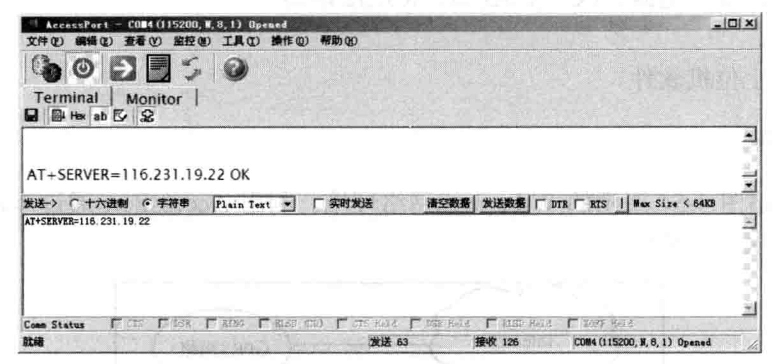


图 4-56　服务器 IP 设置

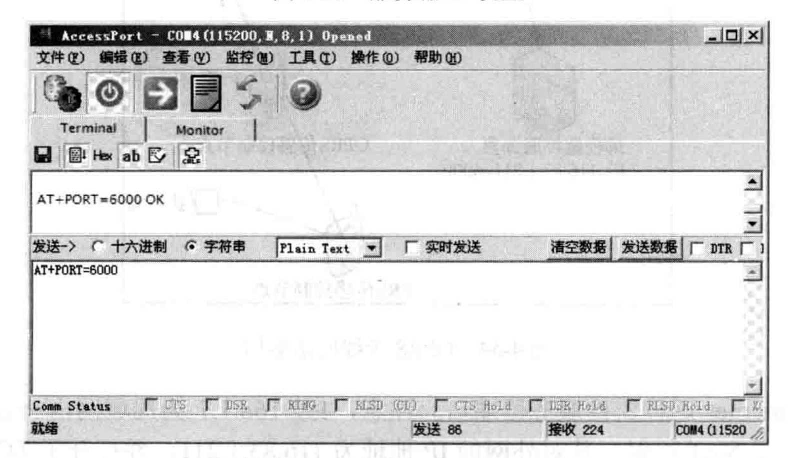
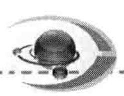


图 4-57　端口设置



（3）启动 GSM 网络，输入指令“AT+GSMON”，并发送。

（4）启动 GPRS 网络，输入指令“AT+GPRSON”，并发送。

（5）重启并保存配置，输入指令“AT+RESET”。

（6）当模块重新启动后，GSM 和 GPRS 网络均已启动成功，如图 4-58 所示。

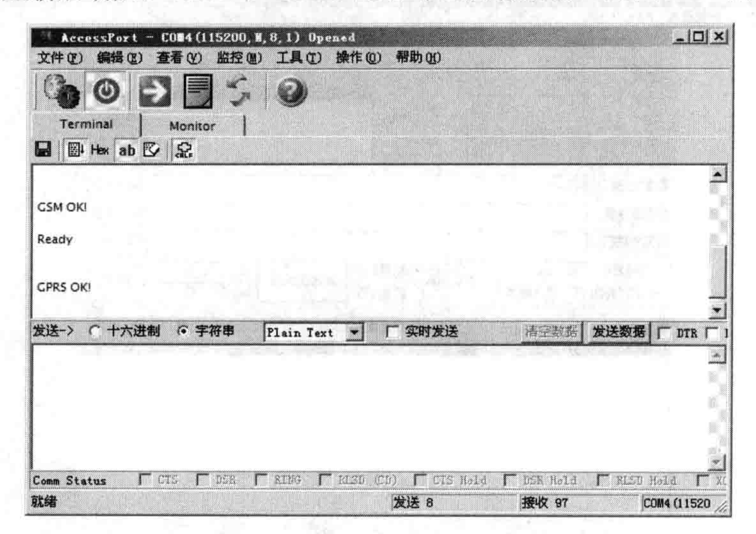


图 4-58　GSM 和 GPRS 网络已启动成功

（7）查看 Internet 远程监控服务器已与 GPRS 节点建立了连接，如图 4-59 所示，表明已经为控制和数据采集做好了准备。这里，仅举几个 GPRS 无线控制与传感数据采集的例子，其余控制与传感数据采集请参考附录二。

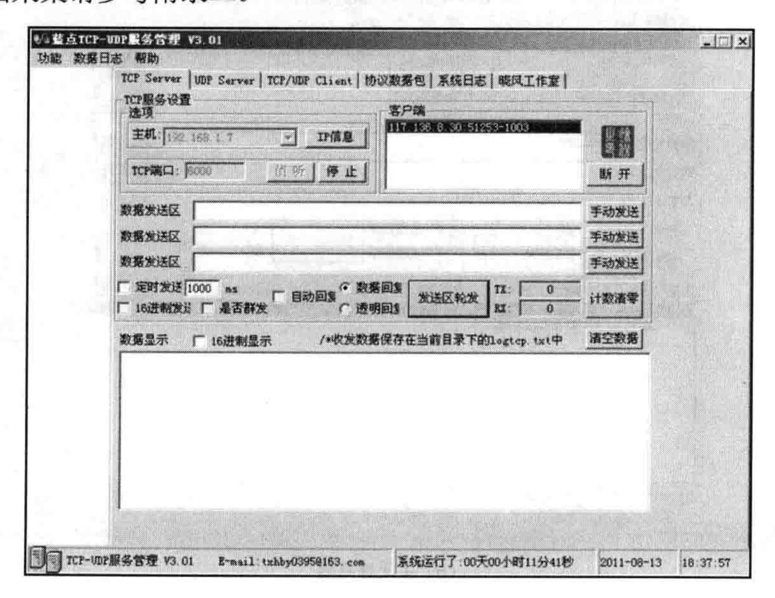


图 4-59　GPRS 节点已连接到远程服务器

步骤 2：控制蜂鸣器。在监控服务器上选择所连接的客户端，在数据发送区输入“BELLON”指令，手动发送，此时 GPRS 节点上的蜂鸣器开始报警；然后再发送停止报警指令“BELLOFF”，此时 GPRS 节点上的蜂鸣器停止报警，如图 4-60 所示。

（a）开启蜂鸣器

（b）关闭蜂鸣器

图 4-60　控制蜂鸣器



步骤 3：控制 LED。选择所连接的客户端，先输入指令“LED1SET”，然后选择十六进制发送，在数据发送中最后输入 EE 控制 LED 灯，手动发送，如图 4-61 所示。注：LED1SET 后面加一个 8 位的十六进制数，8 位分别表示 8 个 LED 灯的状态，对应位为 0 表示亮，1 表示灭。bit0～bit3 对应板载 LED5～LED8，bit4～bit7 对应模块 LED1～LED4。

图 4-61 控制 LED 灯

步骤 4：采集板载温度。选择所连接的客户端，输入指令“DSGET”，手动发送，返回当前板载温度，如图 4-62 所示。

图 4-62 采集板载温度

步骤 5：采集板载光照度。选择所连接的客户端，输入指令“LS1GET”，手动发送，返回当前板载光照度，如图 4-63 所示。

图 4-63　采集板载光照度

4.5　练习题

1．蓝牙组网可依下列步骤完成。

Step 1：____；

Step 2：____；

Step 3：____；

Step 4：____；

Step 5：____；

Step 6：____；

……

其中，设置配对密码命令：______________________________；

设置设备名称命令：______________________________。

配置配对密码时若返回信息：<CR><LF>AT+PINhu1234[空格]ERROR<CR><LF>，说明配置错误。原因是：______________________________________。

模块重启指令是：______________________________________。

2．WiFi 组网可按如下步骤执行。

Step 1：____；



Step 2：____；

Step 3：____；

Step 4：____；

Step 5：____；

Step 6：____；

……

模块重启指令是：______________________________________。

人体感应传感器状态获取指令是：__________________________。

电池电压获取指令是：__________________________________。

板载光敏电阻数据获取指令是：____________________________。

直流电机左转控制指令是：______________________________。

直流电机右转控制指令是：______________________________。

直流电机停止控制指令是：______________________________。

3．GPRS 组网可按如下步骤执行。

Step 1：____；

Step 2：____；

Step 3：____；

Step 4：____；

Step 5：____；

Step 6：____；

……

指定 Internet 远程监控服务器 IP 地址指令是：________________。

指定服务器端口指令是：________________________________。

启动 GPRS 网络指令是：________________________________。

重启并保存配置指令是：________________________________。

步进电机转速设置 300 圈/分指令是：______________________。

CO_2 气体传感器数据获取指令是：________________________。

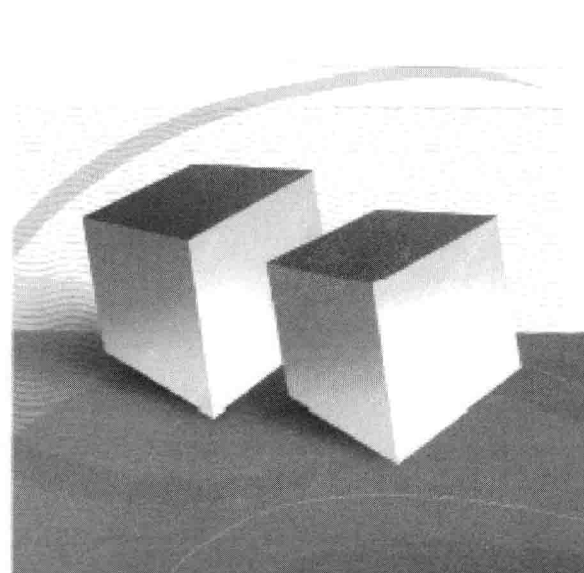
光敏传感器模块数据获取指令是：__________________________。

板载光敏电阻数据获取指令是：____________________________。

第 5 章

物联网工程应用

在掌握了物联网的基本概念及核心技术的基础之上，本章将介绍物联网在零售、安防、通信领域以及智能交通、智能家居、智慧农业、食品和药品中的应用，便于加深对物联网的认识。





5.1　物联网在零售领域的应用

5.1.1　物联网与商品零售概述

世界大型零售企业历来都十分重视采用先进技术，以扩大销售、提高效率和增加利润。现代技术应用于商业和零售业，将大大提升企业的竞争力。创新技术能够提高仓储运输和物流管理的效率。同时，企业将能够为其顾客提供量身定做的服务。

如今的物联网时代，零售企业开始将大量的精力投入到了 RFID 的应用中，不可否认，RFID 作为物联网的支撑技术，它的精确化管理将触角伸到了零售业每一个环节的每一个部件，使得采购、运输、仓储、销售、客户等各方面的管理都变得更加快捷、高效，如图 5-1 所示。

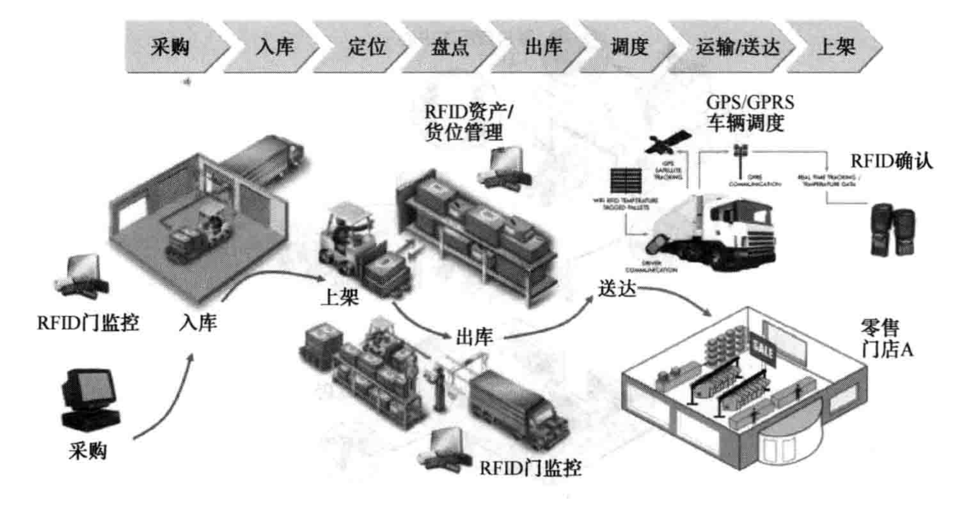


图 5-1　基于 RFID 的产品生命周期管理

5.1.2　物联网零售应用

1. 采购运输

配送中心根据缺货信息向供货商发出需求信息，供货商将贴有 RFID 标签的商品检验后装车运输。在运输的车辆上安装有传感器，可以采集商品的状态信息，包括：温湿度、震动等；通过 GPS 全球定位系统可以对车辆的实时位置进行全程跟踪；运输线上检查点安装有 RFID 接收转发装置，可以接收 RFID 标签反馈的商品装载信息，并将这些信息连同接收地的位置信息通过 3G 等移动通信手段传送给运输调度中心，存入数据库，配送中心就能即时了解商品状态与所处位置，甚至可以确切了解目前有多少箱货处于运输途中、运输的始发地和目的地，以及

预期的到达时间等信息，这都为确认采购计划的实施情况以及下一次采购方案的制定筹划提供了可靠的数据。

2. 配送

配送中心接收到商品后，使用 RFID 读写器对商品进行清点，把读取到的商品信息与采购计划、发货记录等进行核对，如有错漏可以及时更正，同时将当前商品存放地点和状态写入 RFID 标签进行信息记录。当零售门店提出缺货信息后，系统将快速准确地查出所需商品的存放位置，并在所需商品的标签中写入该门店代号，然后装车运输至各个门店，可以避免窜货的现象。此时，RFID 读写器将货物状态更改为出库状态。

到达零售门店的仓库后，安装在仓库入口处的 RFID 读写器会自动扫描商品，在指示存放货架位置的同时将商品信息更改为入库状态。由于商品出入库等配送管理大多是由 RFID 系统自动完成的，从而达到了配送速度提升、配送成本降低、拣选与分发过程的效率与准确率提高的效果，如图 5-2 所示。

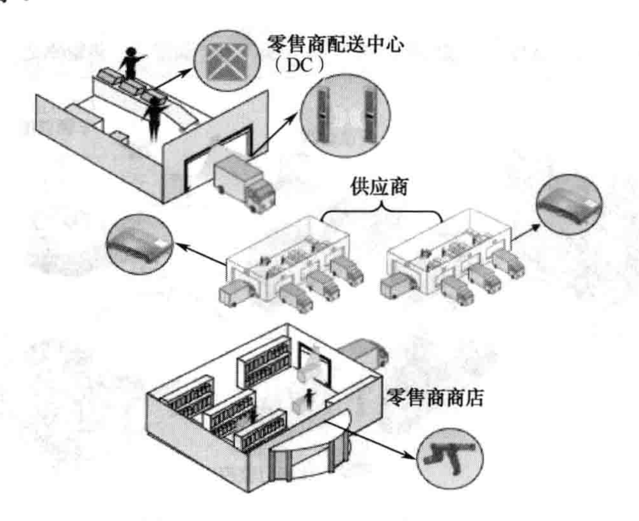


图 5-2　物流配送系统

3. 仓储

将 RFID 与仓库管理系统相结合，可以实现自动化的存货、取货，实时有效地监测库存，对某些时效性强的商品的有效期限进行监控：当产品到保质期或存货不足时，商品的管理系统会及时发出信号，工作人员可以及时补货；当达到存货量的标准时，系统也会发出警告，降低采购量。从而节省了劳动力和库存空间，同时减少了整个物流中由于商品误置、送错、偷窃、损害和库存、出货错误等造成的损耗。RFID 技术的应用也使得商品的登记自动化，盘点时不需要人工的检查或扫描形条码，更加快速准确，进而减少了人力资源的消耗，提高了工作效率，降低了运作成本，如图 5-3 所示。



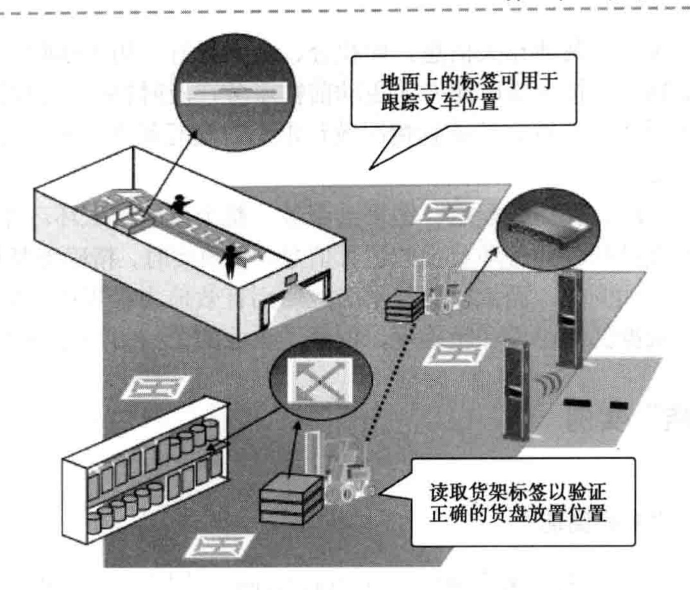


图 5-3　仓储

4. 销售

节假日在结账台前排起的长队是令许多零售商头疼的问题，RFID 可以解决这一问题。顾客在商店购物过程中，安装在店内的 RFID 读写器能自动扫描购物车中的商品信息，并随着顾客购买活动的进行而随时更正，同时货品的信息也会在库存系统中随时更新，当顾客结束购买走向结账台时，系统自动读取、汇总和计费，从而取代了传统的人工条码扫描收费系统，尤其是对于大量多种类购买的顾客，RFID 收费系统的优势将更为突出，它不仅节省了顾客的购物时间，也提高了商店的工作效率，减少了人工条形码识别过程中可能出现的错漏，保证了计费的准确率。

5. 防伪

利用 RFID 对零售商品进行防伪管理，与其他防伪技术相比具有更多优势。每个标签都有一个全球唯一的 ID 号码——UID。UID 是在制作芯片时放在 ROM 中的，无法修改，无法仿造；无机械磨损，防污损；读写器具有不直接对最终用户开放的物理接口，保证了其自身的安全性；因此利用电子标签写入器将货品的重要属性如名称、等级、货号、型号、执行标准、商品编号、检验员编号等写入对应的电子标签，并将该电子标签附加在货品上，每件货品就具有了全球唯一的认证标识，使真品的认证更加准确，有效地遏制了假冒伪劣产品的产生。

6. 客户管理

传统的客户管理服务仅限于会员卡系统，对会员进行统一的促销通知，但在倡导差异化竞争的时代，把细致的服务延伸到每位顾客，实现个性化服务是现代零售业增强竞争力的重要方法。RFID 客户管理系统的运行将对会员卡系统进行有效的个性化服务补充。当顾客进入商店时，商店门口的 RFID 远距离监测系统会自动感应并读取到顾客 RFID 会员卡内的信息，并在商店的液晶屏上显示出针对客户购买习惯的实时促销信息，让顾客对相关信息一目了然；同时

服务系统也会显示出顾客的其他相关信息，如积分、个人喜好、历史购物记录、享受折扣程度等；服务中心可以根据实际情况实时派专人主动前往服务，及时提供有针对性的个性化服务；后台的数据中心也可以将所有顾客的购物情况统计汇总，进行筛选分析，为决策层的重要决策提供准确可靠的数据支持。

零售业从采购、运输、存储、配送、销售到服务，整个供应链上环环相扣，供应链上的成员必须及时获得其他成员和各业务环节上的运行信息，必须实时、精确地掌握整个商流、物流、信息流和资金流的流向和变化，而 RFID 技术的应用则有效地为零售业提供了各项信息数据的监控与跟踪，保证了数据的即时性和精确度，增强了企业的公信力与竞争力。

5.1.3 “未来商店”实例

实例 1：麦德龙“未来商店”

2003 年，麦德龙对外发布“未来商店”（Future Store）计划，并与 50 多家合作伙伴携手开发及测试崭新的应用程序，涵盖零售供应链的各个环节，包括物流及零售门店的顾客体验等方面，如图 5-4 所示。





图 5-4 麦德龙“未来商店”

● 手机购物

体验麦德龙“未来商店”可以通过手机开始。借助 3G 通信技术的飞速发展，顾客所有的购物流程都可以在手机上实现。

顾客打开手机应用，可以通过选择“在超市中”还是“在超市外”获得不同的服务。如果不在超市现场，那么消费者可以通过手机浏览商品信息、促销信息等内容，也可以为下一次到超市购物做些准备。

如果身处超市，只要用手机对着商品条码拍照，就可以获取该商品的价格、保质期等详细信息。如果在家中已经有了一些购物打算，那么在家里就可以通过手机拍摄想购买商品的条码，当顾客来到超市时，手机会自动告知这件商品所处的货架位置，如图 5-5 所示。





图 5-5　手机拍摄条形码

当然，结账也可以通过手机完成，在确定购物完成后，用手机可以生成一个新的条码，只要将这个条码在收银出口的自助收款设备上扫描一下，就可以完成结算，而不用再一件件地扫描商品了。这样购物的速度的确很快，可以让顾客在很短的时间内完成购物过程。

● 智能电子秤

智能电子秤可以更加快捷地为食品称重，智能电子秤上安装了数码摄像机和特殊图像识别软件，通过分析所放物品的质地、颜色和大小，程序会自动识别食品的种类。如果无法确切识别，智能电子秤将显示可能的分类，以便顾客自己选择所放食品的正确种类。智能电子秤称出商品重量并计算价格后，会打印出商品名称、重量、价格和条形码的黏胶标签或 RFID 标签，如图 5-6 所示。

● 智能货架

当商品到达商店时，只要经过一次扫描，就能直接统计出实际到货数量和品种，而省去了拆包一件一件查验的麻烦；商品摆上货架之后，如果出现缺货现象，货架上的 RFID 读写器将立即向后台管理系统发出补货通知；另外，RFID 读写器还可以自动跟踪每种商品的销售速度和销售数量，同时具有安全防盗功能，只要标签中的防窃功能处于激活状态，那么商店出口处的传感器就会报警；当顾客结账时，货物会经过最后一次扫描，同时更新库存，如图 5-7 所示。



图 5-6　智能电子秤



图 5-7　智能货架

实例 2：上海世博“未来商店”

● 世博“未来商店”简介

随着 RFID 射频识别技术在中国的快速发展和推广，麦德龙的“未来商店”对中国来说不再是神话。

坐落于上海市南京东路 558 号的“未来商店”是我国第一个“投入运营”的基于 RFID 技术的未来商店——上海世博会特许商品旗舰店团购中心（见图 5-8），由上海市经济和信息化委员会资助的科技兴贸项目，被列入市经信委迎世博 600 天行动计划。“未来商店”智能购物环境的“心脏”的 RFID 技术是由上海交通大学王东博士携学生完成的。

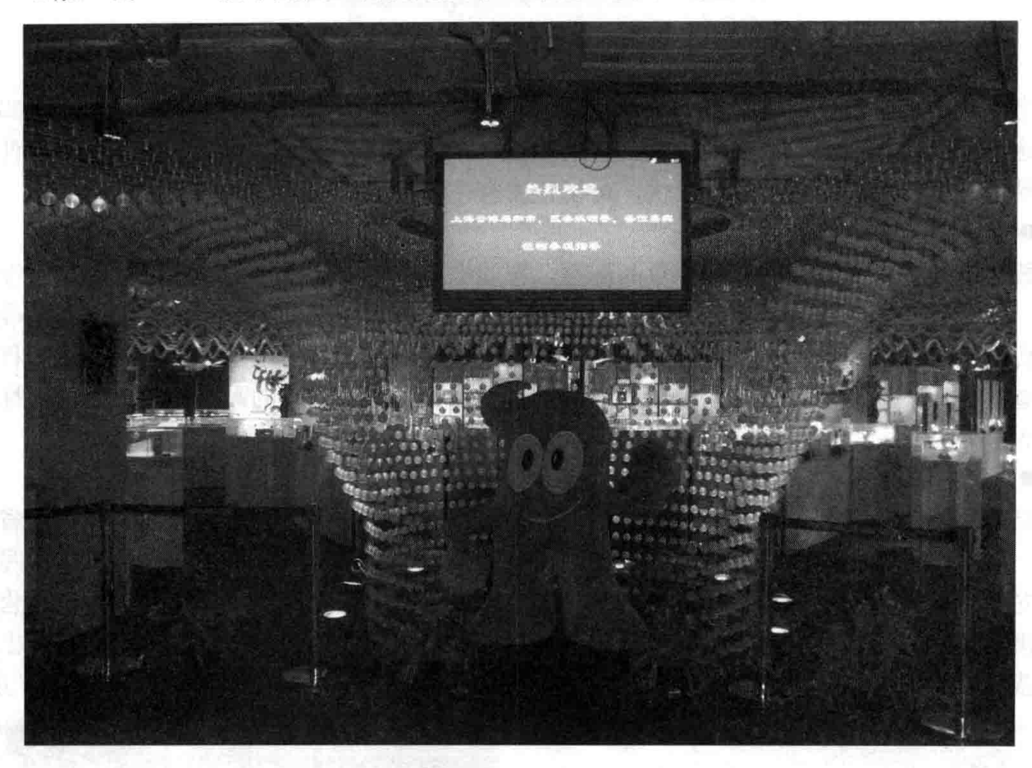


图 5-8　坐落于上海市南京东路的“未来商店”

基于 RFID 技术的“未来商店”在上海早有萌芽，在 2004 年 11 月上海工博会期间，就建立了一家演示性质的 RFID“未来商店”。但是，当时 RFID 技术还有诸多需要解决的问题，比如说 RFID 标签成本很高，所以未来商店不能投入真实的商业运营，商店的开办只是起到科普教育的作用。而随着 RFID 技术的日臻成熟，“未来商店”从科普展示走到正式的商业运营，为顾客提供了前所未有的购物体验。“未来商店”涵盖了均瑶集团的世博特许商品，以及上海新世界旅游纪念品有限公司的旅游纪念品、收藏品等的团购中心和配送中心，实景式展示 RFID 技术应用于商品展示、介绍、销售、物流配送、商业智能等全过程，构建了智能的未来购物环境。

“未来商店”创办的一个关键就是为 RFID 在商业零售领域的应用找到一个真实的场景，通过“巧妙”的商业模式设计和流程运作，在现实应用中既能淋漓尽致地发挥 RFID 技术的优势，



又能弱化正处于持续改善中的 RFID 技术成本和稳定性等问题，在给顾客带来奇妙购物体验的同时，为商家创造了丰厚的利润。RFID 技术应用的商业模式设计和流程运作是一个循环往复的过程，RFID 技术的发展会创造出新的商业应用可能，于是催生新的商业模式设计和流程运作方法，RFID 技术发展与商业应用模式设计保持同步，技术在第一时间被最合理地进行商业化应用，这又会进一步推动技术与应用的发展，形成一个良性的循环。

●“未来商店”物联网系统

首先进入“未来商店”给人的感觉就像进入一个科幻世界。整个商场没有传统的柜台，没有营业员。刚一进门，就会看到商店天花板上波浪起伏的水晶球，设计理念为水晶球波浪起伏的样子就像 RFID 芯片在向外发射信号，巧妙地将 RFID 的概念融入到了商店里。水晶顶下面是一个个玻璃展示柜，展示出琳琅满目的各种高雅、珍贵的商品（见图 5-9）。

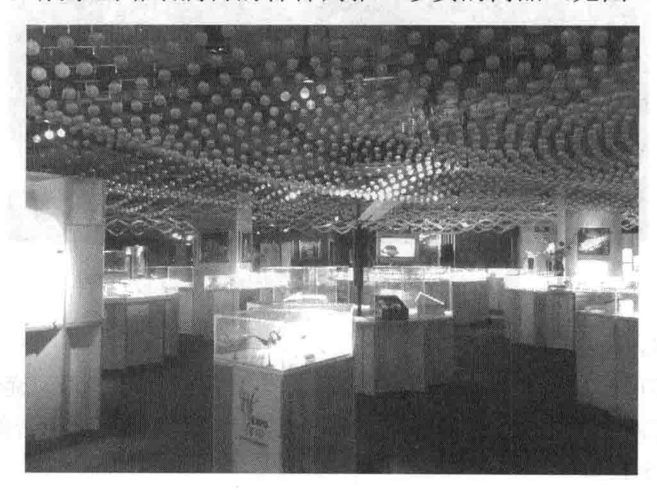


图 5-9 未来商店全景

（1）智能消费卡。

顾客进入世博未来商店后，系统通过读取顾客提交的第二代身份证，获取顾客信息，并且将智能消费卡与顾客的身份证进行绑定，如图 5-10 所示。



图 5-10 智能消费卡与智能手持终端

（2）智能手持终端。

VIP 顾客可以领取一台智能手持终端（见图 5-10）进入商场选购商品。这台手持终端就是随身“导购”。顾客要买任何一款商品，不用从柜台内拿出该商品，只要把智能手持终端对准商品的 RFID 标签，这件商品的介绍、价格等各类信息就会以图像配文字和声音的形式出现在屏幕上，同时配有多种语言介绍，如图 5-11 所示。利用智能手持终端可以把一些具有文化内涵的商品背后的故事，例如作者曲折的创作经历、作品独特的材料和制作工艺等人文和文化底蕴展示出来，这是任何一个营业员或导购人员所不能比拟的。



图 5-11　智能手持终端查询商品信息

（3）旋转广告屏。

在商场内多个环形玻璃柜台的中间均有一台由支架固定、可 360° 旋转的广告屏，顾客将屏幕轻轻挪动至相应商品的上方，该商品的详细介绍将立即以图文及声音的方式显示，可谓“指哪儿读哪儿”（见图 5-12）。

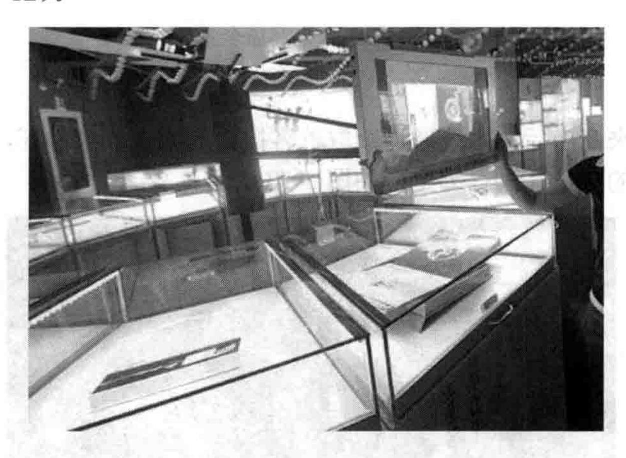


图 5-12　旋转广告屏

而当顾客挑选完商品，掌上电脑上的购物清单会将所选商品名称、单价、数量，一样不缺地显示出来，连总价都为顾客计算好了。在“未来商店”，不会在每件商品上都贴 RFID 标签，而是采用种类标签，为展示柜里的商品贴上 RFID 标签即可，顾客选中哪样商品，想订购多少，库存里都有。顾客只要单击“发送”，订单就会立即传送到后台仓库和结账台。仓库接到订单



后便会立即将货物拣选出来并发到收银台。顾客也可以推着装满商品的购物车经过收银台，不需要像普通超市一样逐一扫描所有商品的条形码，收银台的 RFID 读写器可以在一两秒内自动识读几十件甚至上百件商品的 RFID 标签，购物清单立刻就会呈现在电脑上了。如顾客对某一商品不满意，在掌上电脑上删除即可，非常方便。在结账时，顾客也无须排队，只要在结账时刷一下身份卡，就能读取对应的账单等待支付。世博会期间有大批海内外的游客来购物，如果用传统的一对一模式，营业员肯定不够用，而未来商店却用 RFID 技术巧妙地解除了这些烦恼。

（4）智能购物车。

不过，没有智能手持终端的普通顾客，可以在纸质购物单以外同样体验到智能购物所带来的乐趣，那就是推一辆智能购物车。与普通购物车相比，智能购物车在把手左侧装有一台液晶显示器，消费者可以通过触摸屏的提示，总览商场内所有商品的购买信息。也可根据需要，通过车上延伸出的一台 RFID 读写器就近读取单一商品的信息，如图 5-13 所示。

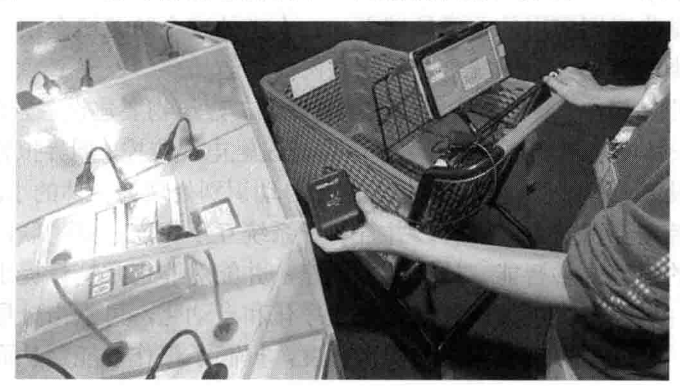


图 5-13　智能购物车

（5）智能结账台。

“未来商店”智能结账台不像普通超市那样，需要收银员逐一扫描每一件商品的条码进行结算，只要消费者推着装有商品的购物车抵达，结账台的读写器便可在一两秒内自动识读几十件甚至上百件商品的标签，购物清单立刻会显示于电脑屏幕上（见图 5-14）。倘若消费者临时决定退还某件商品，收银员则可删除对应的信息，重新结算。

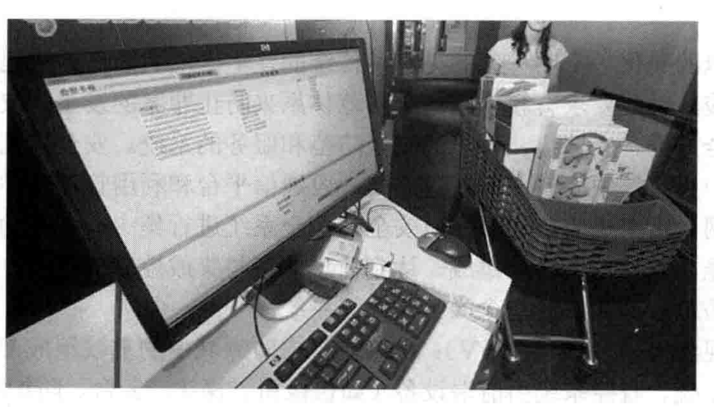


图 5-14　智能结账台

“未来商店”还有很多其他神奇的功能。比如使用智能货架，通过无线价格标签，可以实时动态地修改所有商品的价格信息。顾客只要一拿走货架上的某些商品，后台系统马上就能得到被拿走商品的种类、数量等一系列信息，系统会主动地通知营业员及时补上缺货的商品。此外对于所有进入过“未来商店”的 VIP 顾客，商店的电脑管家还会将顾客的历史购物记录、在商店内的行走轨迹、在某些商品前停留的时间等信息保存到该顾客的个人数据库，利用商业智能技术可以对顾客的信息进行挖掘，为顾客提供个性化的服务。例如可以根据不同顾客的历史购物记录，向顾客有针对性地推荐商品。还可以将顾客停留时间长的商品信息，通过顾客进门时留下的联系方式发送给顾客，实现精准的营销。

5.2 物联网在安防领域的应用

安全防范领域是物联网应用的重要领域之一。人类的安全防范概念很广，我们可以运用各类物联网技术为人类构架起全面的安全防范物联网体系。

首先，大楼及居住小区需要构建智能的安防物联网。建筑物要建设融安防、消防、能源消费管理和智能房屋为一体的建筑物感知体系；小区要建设融电视监控、周界报警、巡更、门禁对讲、灯光广播、防盗与报警、车库管理和小区状态图像自动识别处理为一体的小区安防物联网。

过去的安防监控需要保安紧盯屏幕，并且各子系统互不相连；将物联网技术与安防监控系统整合之后，系统的报警更加智能、处理更加迅速，并能对非正常情景提出对策和告警，自动切换画面跟踪目标，这样各类事件处置能预先程序化和自动化，可点击分层进入查看数据的大屏幕综合图像信息，降低了控制室保安的工作强度，提高了工作效能，从而保障了平安小区的建设。

安防物联网对于案件的及时发现、接警、处置、破案提供了条件，可以有效提高治安效果和公安办案能力，打击犯罪，保障和谐社会，最终将建立起覆盖整个城市的安防社会物联网体系。

因此，通过物联网技术和安防系统的完美组合，可以实现全面的安全管理和安全保护，使得安全管理机构可以全方位监控所有的安全测控点，实现智能安防系统能力的大幅提升。

5.2.1 安全防范自动化

随着城市环境的美化、文明程度的提高，传统的住宅围墙和防盗栅栏已逐步取消，但社会治安形势依然严峻，因此要求有新型的安全防范体系来防止罪案的发生。安全防范自动化系统提供了多层次、全方位、立体化、科学的安全防范和服务的系统。安全防范自动化在住宅安全防范系统的联网中央监控中心室，通过建立同一段通信平台和利用管理软件将中央监控设备与各子系统设备联网，由中央监控中心室对安全防范全系统进行集中或者自动化监控与管理，从而实现设备、功能、软件与网络的集成，达到信息共享与集成控制的目的。

一般的安全防范自动化系统包含如下几个子系统：

（1）闭路电视监控子系统（CCTV）：CCTV 是安防领域中的重要组成部分，是所有安全系统中最关键的子系统。监控系统由前端设备（如摄像机、探头、云台、防护罩、支架、解码器、报警探头、射灯等）和中心控制设备（如硬盘录像机、矩阵主机、监视器、报警盒、视频分配



器等）组成；中心控制设备按照功能划分为硬盘录像系统、矩阵控制系统、报警系统，如图 5-15 所示。系统通过遥控摄像机、探头与云台等辅助设备，直接观察被监视场所的情况，同时可以对被监视场所的情况进行同步录像。另外，电视监控系统还可以与防盗报警系统等其他安全技术防范体系联动运行，使用户安全防范能力得到整体的提高。

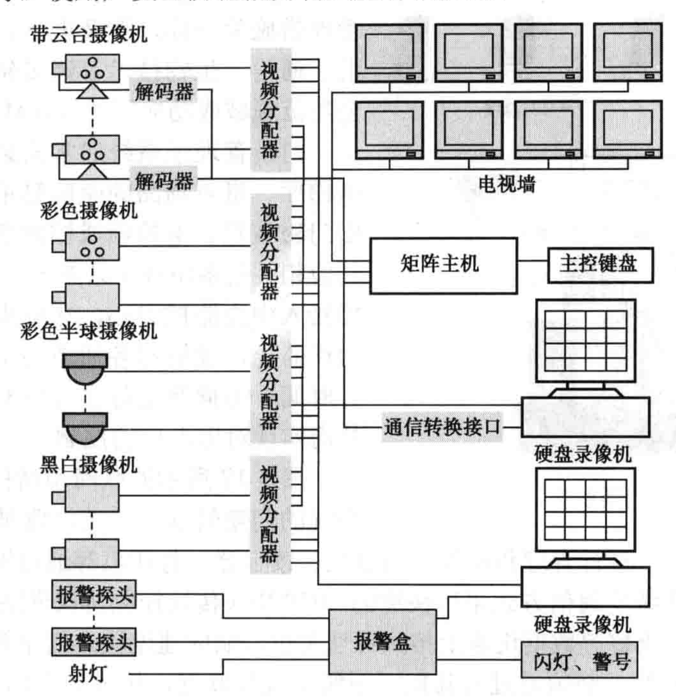


图 5-15　CCTV 监控系统

闭路监控系统能在人无法直接观察的场合，实时且真实地反映被监视控制对象的画面。闭路监控系统已成为广大用户在现代化管理中监控的最为有效的观察工具。在控制中心，只要一个工作人员的操作，就能够观察多个被控区域，以及远距离区域的监控功能。

（2）报警子系统：报警子系统运用现代监测技术，在需要布防入侵的部位或地区周围布置一套物理探测设备，在需要的布防时段启动该系统时，可以在监控中心实时探测到布防区的非法入侵者，对非法入侵者进行实时、可靠和准确无误的报警，不允许漏报。

（3）门禁管理子系统：主要由门禁器（分为磁卡式、按键式、指纹式、声音式、图像式及综合式等）和控制器、数据通信处理器等组成。系统对重要通道、要害部门的人员进出进行集中管理和控制，配合电磁门可自动控制门的开关，并可记录、打印出入人员的身份、出入时间、状态等信息。对未经授权的出入状态，系统将作为紧急报警处理（在接下来的小节里，我们将介绍一种门禁管理子系统解决方案）。

（4）其他子系统：完整的安全防范自动化系统除了必须包含上面几个基本的子系统外，还可以根据需要，包含安保人员电子巡更报警子系统（对安保人员的工作状态进行监测，督促安保人员定时、定点巡视）、停车场管理子系统（对区域内的通行道口实施车辆出入控制、监视、信号指示、停车计费等的管理）。

5.2.2 门禁管理子系统解决方案

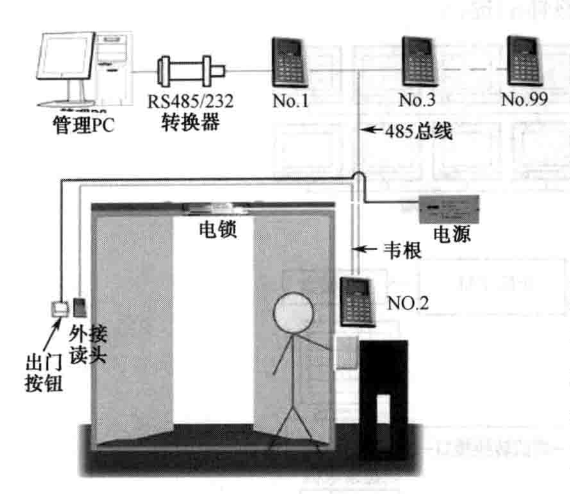


图 5-16 门禁系统

门禁管理子系统融自动识别技术和现代安全管理措施为一体，涉及电子、机械、光学、计算机、通信、生物技术等诸多领域，是物联网在安全防范领域成功应用的具体体现。

门禁管理子系统通常安装在主要的出入口、电梯厅、贵重物品的库房等重要部门的通道口，由门磁装置、电控锁或控制器、读卡器、电源盒其他相关设备组成（见图 5-16），设备通过网络连接接入中央监控中心，在中央监控中心通过门禁软件监控，能够对各通道的位置、通行对象及通行时间、方向等进行实时控制或设定程序控制，从而实现对出入口的控制。

图 5-17 所示的联网型结构的安全防范自动化系统的门禁管理子系统经常被采用，系统由中央监控中心的计算机统一进行管理和控制，门禁机、读卡器、打印机等通过网络接入中央监控中心，构成物联网。系统的通信方式采用快速的 TCP/IP（传输控制协议/网际协议）双向通信模式，使得指纹图形、报警等数据迅速上传到管理主机，响应速度快。门禁管理只是安全防范自动化系统的一个子系统，必须通过与其他子系统集成和联网，构成更大的“物联网”，才能成为整个安全防范自动化系统有效运行的保证。

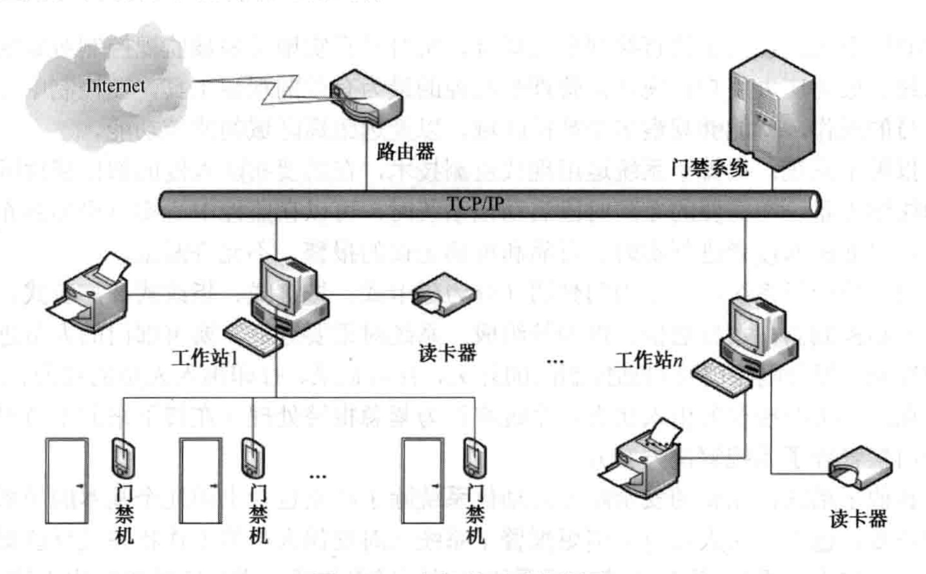


图 5-17 安保联网型结构图



5.2.3 上海浦东国际机场防入侵物联网系统

2009 年 7 月 1 日，《民用机场管理条例》将正式实施，新条例对机场的安全运营提出了更高的要求，与此同时各机场也在不断地努力和探索更高的安全技术。

在上海浦东国际机场（简称浦东机场，见图 5-18）某段围界外，两名“全副武装”的“飞行爱好者”鬼鬼祟祟地走近防护网，商量着如何翻越高高的防护网进入机场，但他们还未靠近防护网，就被一阵阵警告声给吓退了回去。随后，两人又尝试了从外围挖掘、翻越旁边的防护墙等各种方法，均被警告声制止，就在两人犹豫着下一步行动之时，几名安保人员突然出现，将他们“擒”住……

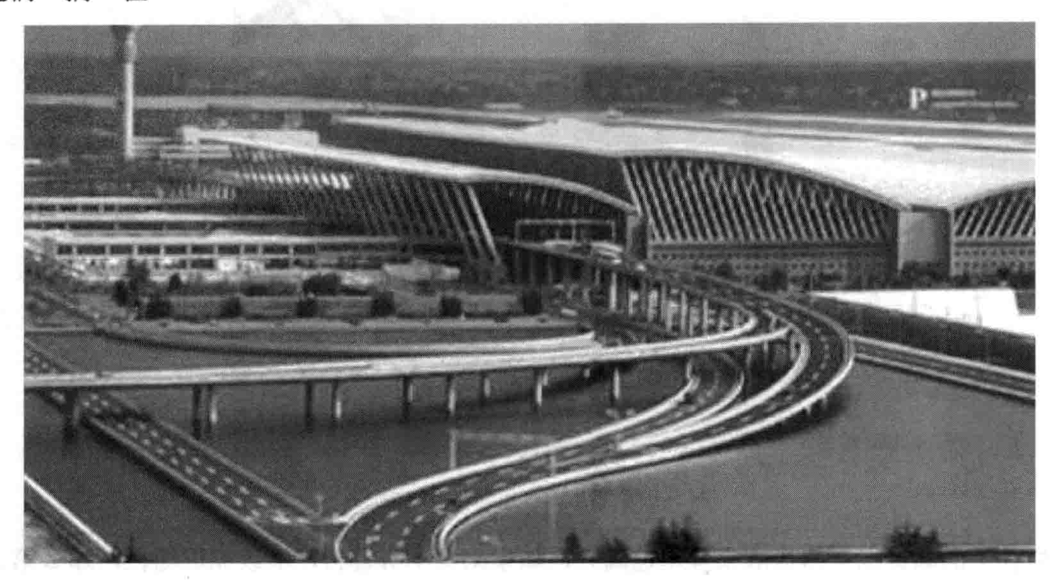


图 5-18 美丽的上海浦东国际机场外景

上述场景并非真实发生，而是浦东机场向来自全国 20 多个机场的安全技术人员，演示其新投入使用的最新一代的围界防入侵系统，展示了我国机场围界安全在“技防”方面的新突破。

从 20 世纪 90 年代中后期开始，一些机场开始将多种技术手段引用到防入侵系统，这些技术包括振动光纤、辐射电缆、红外对射、张力围栏、高压脉冲等。这些“信号驱动”型技术各有所长，对机场安防水平的提高有一定的促进作用。可是，这些单一的技术手段难免存在缺陷，有的受气候条件干扰严重，有的存在监控死角，漏警、误警现象频繁发生。因此，无法实现全天候、全天时、立体化的实时监控和防护。

由于上述原因，特别是误警现象频繁的发生，目前一些采用“信号驱动”围界安防技术的机场大多已经停用了该系统，如广州新白云国际机场、沈阳桃仙国际机场、大连周水子国际机场等。现在，利用物联网就可以解决机场安全防范面临的各种问题。

2009 年，由无锡传感网中心开发的传感安全防护系统在上海浦东国际机场和上海世博会被成功应用，该系统采用一种“目标驱动”型安全防范技术，由 10 万个微小的传感器组成，这

些传感器散布在墙头、墙角、墙面和周围道路上，构成强大的协同感知“物联网”，可实现全新的目标识别、多点融合和协同感知，对机场入侵目标进行有效分类和高精度区域定位，防止人员的翻越、偷渡、恐怖袭击等攻击性入侵行为。

如图 5-19 所示，浦东国际机场围栏外有一道无形的网，这个网由埋设在地下的传感器组成。这些传感器能够根据声音、图像、振动频率等信息分析判断爬上墙的究竟是人还是猫狗等动物，识别目标是什么，同时识别出物体的行为方式，比如说当物体接近栅栏时，系统能识别是人还是车辆，是人在爬栅栏，还是风在吹栅栏，或是鸟停在栅栏上面晃动。不仅如此，系统还能精确地进行定位，一旦发现有人靠近栅栏，系统就会自动发出善意提醒——“机场禁区，请迅速离开，机场禁区，请迅速离开。”



图 5-19 浦东国际机场的电子围栏

栏杆上的高音扬声器提醒来者迅速离开，如果来者不听警告，继续靠近栅栏，那么第二道防线就会报警。

在铁栅栏里面，还有第三道电子传感围界，只要人员进入到机场的铁栅栏里面，报警系统也就相应提高到最高级别。这些传感器节点与机场控制大厅紧密相连。安全防范系统通过几个传感器的协同感知，确定来者位置，机场控制大厅里面的显示屏所对应的警务分片区就立刻变红闪烁，工作人员单击红色区域进去打开监控视频，就能知道来者在做什么，进而采取行动。通过这些无形的传感网络，机场控制大厅就能够迅速对出现的报警情况进行处理。

自从美国发生“9•11”事件后，安全问题成为人们日益关心的话题。而物联网在安全防范领域是可以大显身手的，为人类营造安全的环境，对于提升人们的安全感有着重要的意义。

5.3 物联网在通信领域的应用

手机已经成为我们每个人日常生活必须携带的物品。据国际电信联盟（ITU）统计，截至 2009 年底，全球手机用户达 46 亿，手机普及率超过 50%。到 2010 年，中国的手机用户数量将达到近 7.4 亿，是全球使用手机人数最多的国家。随着手机的普及，移动通信终端将成为主要



联网工具，是未来物联网的重要组成部分。

现阶段，物联网在移动通信领域的应用主要以M2M（Machine to Machine）的形式展开。M2M 是一种理念，也是所有增强机器设备通信和网络能力的技术的总称，它作为实现机器与机器之间的无线通信手段，使人与人（Man to Man）、人与机器（Man to Machine）、机器与机器（Machine to Machine）之间畅通无阻，使随时随地通信成为可能。

随着各种通信技术从平行、独立地发展，逐步走向融合，通过 M2M 相关产业正式纳入国家《信息产业科技发展“十一五”规划和2020年中长期规划纲要》重点扶持项目。

下面将介绍物联网在移动通信中移动支付应用和世博“手机票”的应用。

5.3.1　移动支付

2010 年 9 月 15 日，中国银联与原铁道部签署战略合作协议，使用手机、电话、互联网、自动售票机等新兴支付方式购买火车票成为可能。图 5-20 为北京中国银联工作人员向观众介绍手机支付功能。

2010 年 7 月底，深圳市轨道交通建设指挥部宣布，继市民实现坐公交“刷手机”乘车后，市民坐地铁也可实现“刷手机”支付；而早在上海世博会开园时，游客只要去移动营业厅换张手机 RFID-SIM 卡，不仅可以直接刷手机进入世博园，还能在园内刷手机吃饭、买饮料以及乘坐地铁，如图 5-21 所示。



图 5-20　银联工作人员介绍手机支付功能

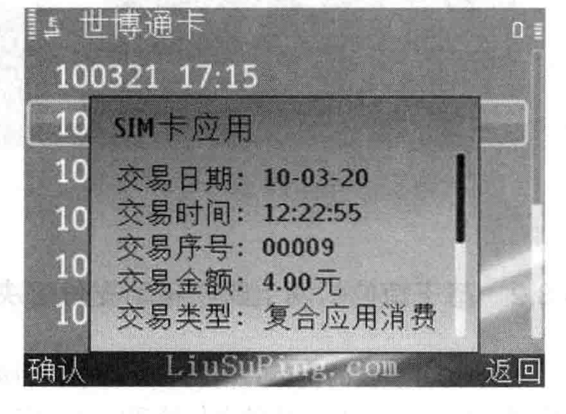


图 5-21　世博 RFID-SIM 卡支付记录

手机支付技术，让手机变成了“钱包”、“钥匙”、“门票”，甚至更多。

手机支付是移动支付（Mobile Payment）的一种重要支付方式，是物联网在金融领域的典型应用。目前国内市场上，中国移动、中国电信、中国联通 3 家运营商和中国银联在积极推广各自的手机支付应用方案。

移动支付是移动通信网和 Internet 的有机结合，作为一种移动增值业务，尽管只是最近几年才发展起来的支付方式，但因其有着与信用卡同样的方便性，同时又避免了在交易过程中使用多种信用卡以及商家是否支持这些信用卡结算的麻烦，消费者只需一部手机，即可完成整个交易，不仅为消费者提供了更大的便利性，也为运营商和商家带来了巨大的商机。

整个移动支付系统通过网络，将移动运营商、支付服务商（如银行、银联等）、应用提供商（如网上商店、公交、校园等）、设备提供商（如终端厂商、卡供应商等）和终端用户等实体联系在一起，行成一个巨大的物联网，基于这个“物联网”完成价值的“转移”。

国内目前使用的手机支付主流技术方案有三个：基于 2.4GHz 的 RFID-SIM 卡方案、基于 13.56MHz 的非接触技术的 NFC 方案和基于 13.56MHz 技术的贴片卡方案。其中，基于 RFID-SIM 卡方案由中国移动主导、国内企业自主研发，在技术上具有后发优势，带宽大、速率高。

而中国电信推出的手机支付业务“翼支付”是将钱包账户置入天翼手机的 RF-UIM 卡中，用户持天翼手机可以在超市、便利店、商场等特约商户购物；中国联通的手机支付方案采用定制手机，并把原有 SIM 卡更换成 SWP-SIM 卡，即能实现在便利店、餐饮店进行现场刷卡。

根据支付时支付方与受付方是否在同一现场，可以将移动支付分为远程支付和现场支付。如通过手机进行网上购物就是远程支付，而通过手机在自动售货机上购买饮料则是现场支付（需要特制的 RFID-SIM 手机卡，见图 5-22 和图 5-23）。

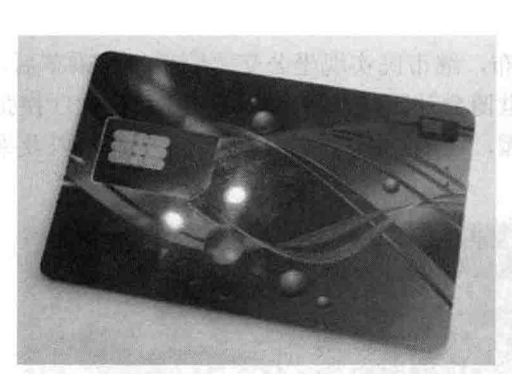


图 5-22　RFID-SIM 手机卡



图 5-23　使用移动支付现场支付购买饮料

5.3.2　基于短信的网上购物移动支付解决方案

移动支付涉及的主体有消费者、移动支付处理中心、商家以及支付服务提供商（银行），如图 5-24 所示。其中，移动支付处理中心是整个支付处理系统的核心，负责联系系统中的其他实体，提供支付处理服务。同时，移动支付处理中心还维护用于认证的用户信息及认证服务。移动支付处理中心实现了提供管理与消费者、商家和支付服务之间的交互。通常移动支付处理中心可以由移动运营商来实现。支付服务提供商（银行）向移动支付处理中心提供支付服务。

一种基于手机短信进行网上购物的移动支付业务流程包括：

（1）用户登录网上购物商务网站，进行注册。

（2）用户凭注册的用户身份登录网上购物商务网站。

（3）选择欲购买的商品，然后确认使用移动支付处理中心的“移动支付平台”进行支付；网上购物商务网站根据用户提交的购物和支付方式请求，生成购物确认短信，包含一个消费确认码（随机产生），发送至用户的手机。





图 5-24　移动支付流程

（4）用户收到消费确认码后，需要在网页上同时输入移动支付账户的交易密码和消费确认码，确认支付。

（5）支付请求由网页提交网上购物商务网站处理服务器。

（6）网上购物商务网站根据用户的购物情况，向移动支付平台发送“支付请求”。

（7）支付平台经过身份校验，扣费成功后，将“支付响应”返给网上购物商务网站。

（8）网上购物商务网站收到对应的支付平台的扣费成功响应后，在网页上显示购物支付成功，同时通过短信通知手机用户；移动支付平台交易成功后，主动发送扣费通知给手机用户（必需的步骤，可以防止网上购物商务网站的一些恶意扣费情况）。

5.3.3　世博“手机票”

第 41 界世界博览会（简称世博会）于 2010 年 5 月 1 日至 10 月 31 日在中国上海举办。这次世博会的主题是“城市，让生活更美好”（Better City，Better Life）。为了响应这个主题，让人们真正享受到“城市科技的创新”，上海世博局联合中国移动于 2009 年 10 月 13 日发布了世博会历史首创的“世博手机票”，将物联网技术成功应用于移动通信领域。

世博“手机票”把 RFID 技术与中国移动 SIM 卡相结合，手机用户可以保持原号码不变，只需更换一张特殊的 RFID-SIM 卡，并在人工售票终端上（见图 5-25 和图 5-26）进行操作购买门票，购票成功后，“手机票”便以一条特殊的信息形式下载到 SIM 卡中。通过物联网，用户就不用拿着传统的纸质门票，而是掏出手机在世博园区入口检票处安放的专用读取设备上轻轻一挥，便完成了检票程序，如图 5-27 和图 5-28 所示。

除了用作“手机票”，在世博会期间和世博会后，持这种 RFID-SIM 卡的手机用户还可以在上海世博园区内进行小额支付、就餐、购物等大众消费，以及乘坐地铁，享受科技带来的时尚、便捷的生活。图 5-29 显示了世博“手机票”系统原理及拓展功能。



图 5-25　世博“手机票”移动售票终端



图 5-26　手机定制世博门票



图 5-27　世博园入口三辊闸可检验手机票



图 5-28　工作人员示范

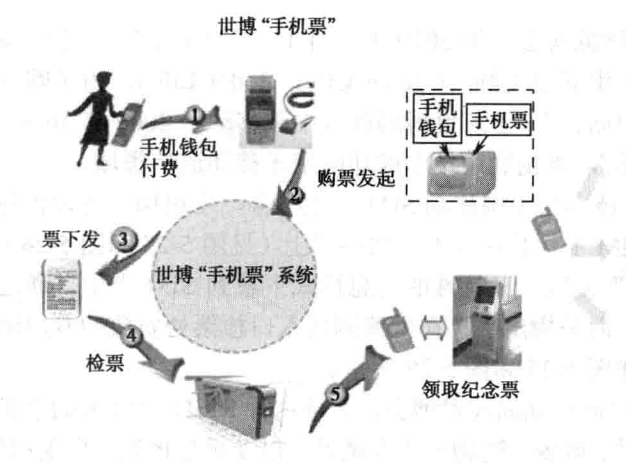










图 5-29　“手机票”的工作原理及拓展业务



移动支付业务作为移动增值业务的一种业务形式，不仅可以给用户带来极大的便利，还可以给运营商以及服务提供商带来增值收益。随着网络带宽的增加、网络技术的提高和安全协议的逐步成熟，移动支付业务的应用会越来越广泛，其发展前景一定会更加广阔。

5.4 物联网在智能交通领域的应用

物联网可以很好地应用到诸多领域，智能交通领域即是其中之一。目前的智能交通系统（Intelligent Transport System，ITS）是21世纪现代交通运输体系的发展方向，主要包括以下几个方面：先进的交通信息服务系统、先进的交通管理系统、先进的公共交通系统、先进的车辆控制系统、先进的运载工具操作辅助系统、先进的交通基础设施技术状况感知系统、货运管理系统、电子收费系统和紧急救援系统。

5.4.1 物联网智能交通概述

智能交通系统 ITS 将先进的传感器技术、RFID 技术、无线通信技术、数据处理技术、网络技术、自动控制技术、视频检测识别技术、GPS 技术、信息发布技术等综合运用于整个交通运输管理体系，通过对交通信息的实时采集、传输和处理，借助各种科技手段和设备，对各种交通情况进行协调和处理，建立起一种实时、准确、高效的综合运输管理体系，从而使交通设施得以充分利用，并能够提高交通效率与安全，最终使交通运输服务和管理智能化，实现交通运输的集约式发展。

从上面可以看出，智能交通与物联网的结合是必然的，智能交通行业已被公认为是物联网产业化发展落实到实际应用的最能够取得成功的优先行业之一，必将能够创造出巨大的应用空间和市场价值。

以往的交通控制是被动式的，主要以环形线圈和视频为主要手段进行车流量检测；而物联网时代的智能交通，则全面涵盖了信息采集、动态诱导、智能管控等环节。通过对机动车辆信息和路况信息的实时感知和反馈，在 GPS、RFID、GIS 等技术的集成应用和有机整合的平台下，实现了车辆从物理空间到信息空间的唯一性双向交互式映射，通过对信息空间的虚拟化车辆的智能管控，实现对真实物理空间的车辆和路网的“可视化”管控。

例如：道路物联网通过与电子车牌、自动防撞驾驶系统和车辆物联网结合，可实现大流量快捷的安全交通。同时在道路中埋设各种传感器和信息交互器，能感知路面车辆的速度、方向以及车道，还能识别车辆的车牌号码、驾驶员姓名以及行车状况。另外，道路物联网还能发出限速要求、车道停车、车辆方向等指令，配合车辆之间的信息交互和定位测速。

作为物联网感知层传感器技术的发展，实现了车辆信息和路网状态的实时采集，从而使得路网状态仿真与推断成为可能，更使得交通事件从“事后处置”转化为“事前预判”这一主动警务模式，是智能交通领域管理体制的深刻变革，如图 5-30 所示。

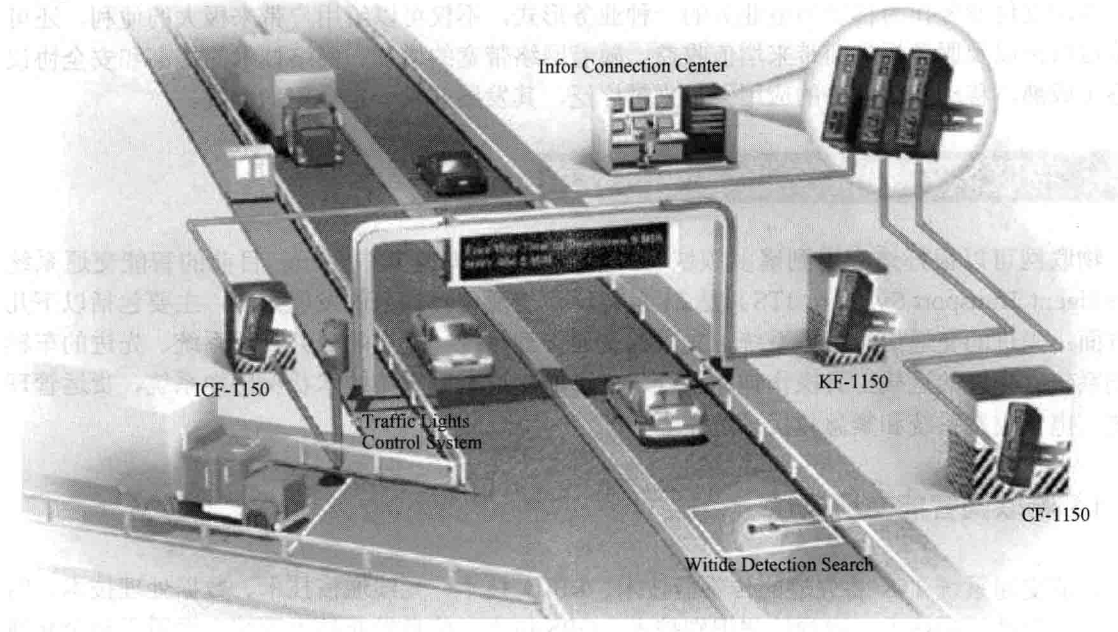


图 5-30　智能交通

5.4.2　ETC 收费系统简介

不停车收费系统是智能交通的重要组成部分。随着交通车辆的不断增加（见图 5-31 和图 5-32），传统人工收费方式的缺点逐渐凸显，严重影响收费站的通行能力。科技的发展使得联网收费成为可能，不停车收费的呼声越来越高。

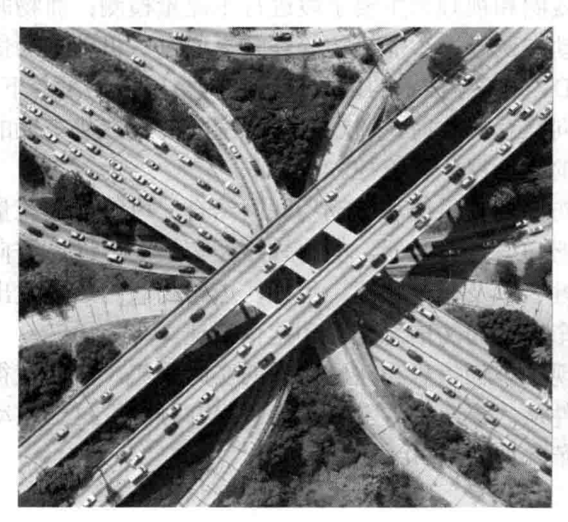


图 5-31　高速公路上川流不息的车流



图 5-32　繁忙的首都机场高速收费站



1. 何为 ETC

ETC（Electronic Toll Collection）是不停车电子收费的简称，又称电子收费系统，是 ITS 的重要组成部分。ETC 系统是一种能实现不停车收费的全天候智能型分布式计算机控制、处理系统，是电子技术、通行和计算机技术、自动控制技术、传感技术、交通工程和系统工程的综合产物，是典型的物联网应用。它利用专用短程微波通信技术，通过路侧单元（Road Side Unit，RSU）与车载单元（On board Unit，OBU，即放在车上，用来和路边架设的 RSU 通信的微波设备）的信息交换，当车辆高速通过 RSU 的时候，OBU 和 RSU 之间用微波通信，就像我们的非接触卡（10 厘米，13.56MHz）一样，只不过距离更远（十几米），频率更高（5.8GHz），通过的时候，自动识别车辆，获得车型，计算费率。采用电子支付方式，自动完成车辆通行费扣除的全自动收费方式。图 5-33 为 ETC 系统的简易工作示意图。

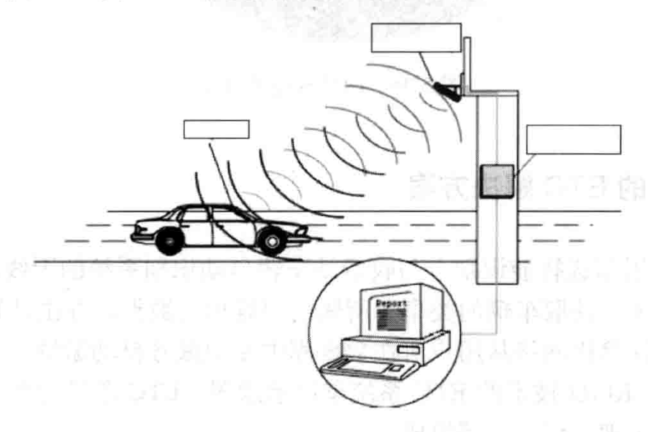


图 5-33　ETC 结构图

当 ETC 系统检测到车辆进入 ETC 车道的时候，安装在龙门架上的微波天线与安装在汽车挡风玻璃上的“电子标签”自动进行信息交换，与微波天线相连接的 ETC 车道计算机根据电子标签中存储的信息识别出车辆信息，并根据车主的使用情况从其银行账号中扣除通行费。交易成功后，车道栏杆自动升起，放行车辆；车辆通过后，栏杆自动降下。整个收费过程无须人工干预，用户可不停车快速通过 ETC 收费车道。

2. ETC 系统的关键设备

微波专用短程通信设备是 ETC 系统的关键设备，它主要由微波天线和电子标签两大部分组成。电子标签按形态可分为单片式和两片式两种。单片式电子标签在物理结构上是一个不可拆分的整体，既存储了车牌号、车型等车辆物理参数，也记录了用户的消费账号、账户金额方面的信息。

两片式电子标签则由固定安装的车载机和可插拔的支付卡（双界面 CPU 卡）两部分组成，车载机里存储了车牌号、车型等车辆物理参数，而用户的消费账号、账户金额方面的信息则存储在支付卡里面。

两片式电子标签的实物如图 5-34 所示。图中的粤通卡为广东省使用的专用支付卡。

车载机（OBU）安装在车辆的挡风玻璃前，具有防拆卸功能，非法拆卸会使 OBU 失效，需要重新发行后才能使用。

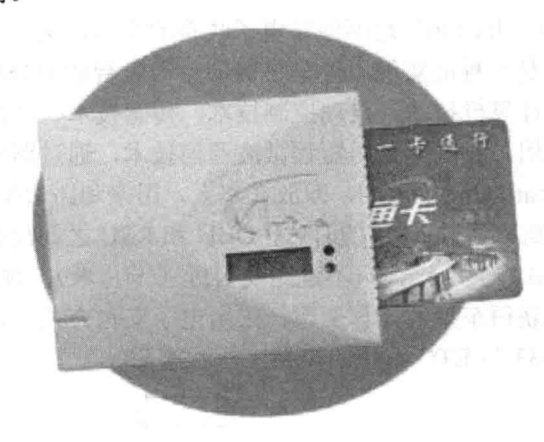


图 5-34　两片式电子标签

5.4.3　基于 RFID 的 ETC 解决方案

ETC 的关键是利用车载智能识别卡与收费站车辆自动识别系统的无线电收发器之间，通过无线电波进行数据交换，获取车辆的类型和所属用户等相关数据，并由计算机系统控制指挥车辆通行，其费用通过计算机网络从用户所在数据库中专用账号自动缴纳。

图 5-35 为某基于 RFID 技术的 ETC 系统车道示意图。ETC 车道主要由天线、地感线圈、自动栏杆、收费额显示牌、信号灯等组成。

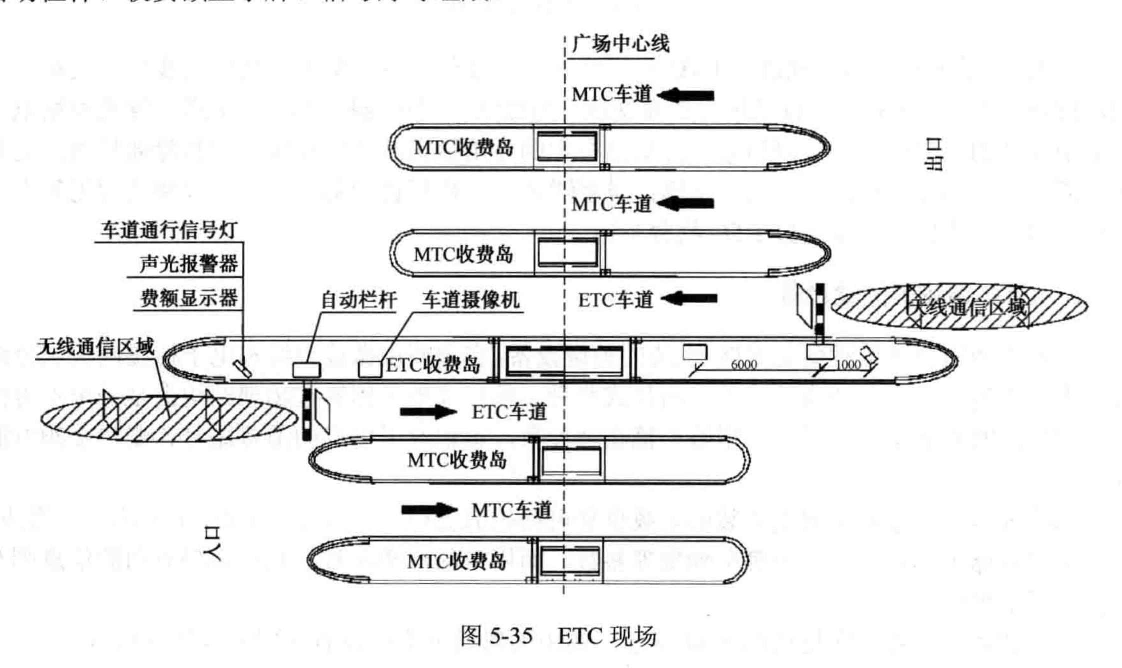
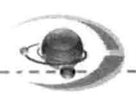


图 5-35　ETC 现场



ETC 系统的工作流程如下。

如图 5-36 所示，ETC 车道的过车原理如下：

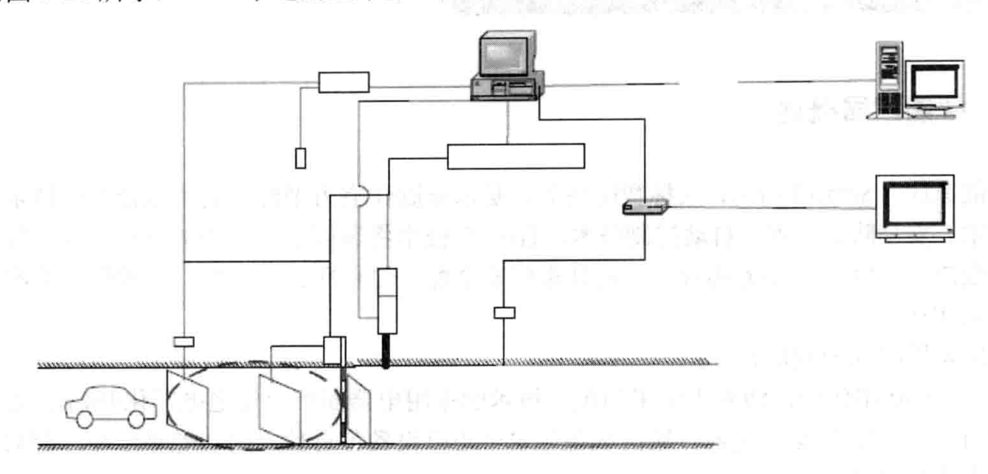


图 5-36　ETC 三个模块

（1）车辆进入通信范围时，首先压到触发线圈，启动读写天线。

（2）读写天线与电子标签（车载机＋CPU 卡）进行通信，判别车辆电子标签是否有效，如有效则进行交易；无效则报警并保持车道封闭，直到车辆离开检测线圈。

（3）如交易成功，系统控制栏杆抬升，通行信号灯变绿，费额显示牌上显示交易信息。

（4）车辆通过抓拍线圈时，系统进行图像抓拍，字符叠加器可将过车信息叠加到抓拍图像中。

（5）车辆通过落杆线圈后，栏杆自动回落，通行信号灯变红。

（6）系统保存交易记录，并将其上传至收费站服务器中，等待下一辆车进入。

整个 ETC 系统分为数据采集模块、数据传输模块、后台数据处理模块三个部分。

（1）数据采集模块：采用 RFID 技术，主要由 RFID 车载超高频无源射频标签和电子读头设备、高速长距离超高频阅读器组成。RFID 可以采取非接触的射频通信方式，通过读写器与标签的无线通信实现数据采集，识别标签载体的身份等特征。

（2）数据传输模块：以高速公路光纤网作为基础、无线网络为补充的数据传输方案。

（3）后台数据处理模块：负责基础数据的管理、系统安全管理、费用运算、路径运算、通行费拆分、系统相关报表管理等，以及车载电子标签联名卡的办理、代扣通行费等金融方面的服务。

系统的三个模块组合在一起，实现 ETC 功能。

将先进的信息技术、数据通信技术、电子控制技术及计算机处理技术综合，有效地运用于公路运输管理系统，构成强大的交通“物联网”，将成为 21 世纪现代化运输体系的基本模式和发展方向，也是交通运输现代化的一个重要标志。

5.5 物联网在智能家居领域的应用

5.5.1 智能家居概述

智能家居（Smart Home）又称智能住宅，是以家庭住宅为平台，利用综合布线技术、网络通信技术、安全防范技术、自动控制技术、音/视频技术将家居生活有关的设施集成，构建高效的住宅设施与家庭日常事务的管理，提升家居安全性、便利性、舒适性、艺术性，并实现环保节能的居住环境。

智能家居概念的起源很早：

20 世纪 80 年代初，随着大量采用电子技术的家用电器面市，住宅电子化开始出现。

80 年代中期，将家用电器、通信设备与安全防范设备各自独立的功能整合在一起后，形成了住宅自动化概念。

至 80 年代末，由于通信与信息技术的发展，出现了通过总线技术对住宅中各种通信、家电、安防设备进行监控与管理的商用系统，这在美国被称为 Smart Home，也就是现在智能家居的原型。

进入 21 世纪后，智能家居的发展变得多样化，技术实现方式也更加丰富。总体而言，智能家居发展大致经历了四代：

第一代主要是基于同轴线、两芯线进行家庭组网，实现灯光、窗帘控制和少量安防等功能。

第二代主要基于 RS-485 总线，部分基于 IP 技术进行组网，实现可视对讲、安防等功能。

第三代实现了家庭智能控制的集中化，控制主机产生，业务包括安防、控制计量等业务。

第四代基于全 IP 技术，终端设备基于 ZigBee 等技术，智能家居业务采用“云”技术，并可根据用户需求实现定制化、个性化。

目前智能家居大多属于第三代产品，而美国已经对第四代智能家居进行了初步的探索，并已有相应产品问世。

近年来，物联网的发展为智能家居引入了新的概念及发展空间，智能家居也是物联网的重要应用领域。基于物联网的智能家居表现为利用信息传感设备（同居住环境中的各种物品松耦合或紧耦合）将家居生活有关的各种子系统有机结合在一起，并通过网络进行连接，实现监控、管理信息交换和通信的家居智能化。主要包含八大子系统：家居照明控制子系统、家庭安防子系统、家庭环境控制子系统、背景音乐子系统、家庭娱乐子系统、家庭能量管理（三表抄送）子系统、家庭自动化子系统和家庭信息处理子系统。

5.5.2 智能家居现状

自 1984 年世界上第一幢智能家居在美国建成以来，欧美和东南亚等经济比较发达的国家先后提出了各种智能家居的方案。智能家居在美国、日本、德国、法国、韩国的广泛应用，为世界范围内智能家居产业标准制定和业务模型探索起到了至关重要的作用。



美国智能家居以数字家庭和数字技术改造为契机，偏重于豪华感，追求舒适和享受，但其能源消耗很大，与低碳、环保的理念相悖。日本的智能家居是开发设计、施工规模化与集团化，以人为本，注重功能，兼顾未来发展与环境保护，大量采用新材料、新技术，充分利用信息、网络控制与人工智能技术，实现住宅技术现代化。德国的智能家居追求专项功能的开发，注重基本的功能性。韩国政府对智能小区和智能家居采取多项政策扶持，规定在首尔等大城市的新建小区必须具有智能家居系统。目前韩国全国 80%以上的新建项目采用智能家居系统，催生了三星、LG 等智能家居品牌。

我国智能家居产业中北京、上海、深圳发展相对超前。深圳的智能家居在布线方面做得比较好，前瞻性较强，考虑电源、空调、电话、电视、网络等方面较周全，预埋智能布线的观念比较超前；北京的智能家居在考虑功能和地方风格方面做得比较好；上海浦东新城区的城区规划和小区布置更符合上海这样一个商业化大都市的需求。青岛海尔和霍尼韦尔的示范应用值得借鉴。青岛东城国际作为 U-home 智能家居示范项目，曾在 2008 年底让前 1000 户业主享受到了 U-home 智能系统带来的便利与舒适，如图 5-37 所示。



图 5-37　海尔 U-home 智能家居

5.5.3　智能家居系统解决方案

在室内有各种家用电器、家用机器人等，采用多种传感器对室内环境进行监测；布有以太网、电导线，使得各种家庭设备接入智能家居网关，同时可以通过 WiFi、ZigBee 等无线传输信号，使用遥控器控制相应的设备。在室外，可以通过 Internet 或者手机进行远程访问控制，如图 5-38 所示。

该智能家居系统具有如下功能：

（1）对灯管照明设备进行智能化控制。

（2）对空调、冰箱、电热水器等家用电器进行智能化控制。

（3）通过各种传感器、探测器，对厨房、卫生间等容易发生安全隐患的区域进行自动监控和报警。

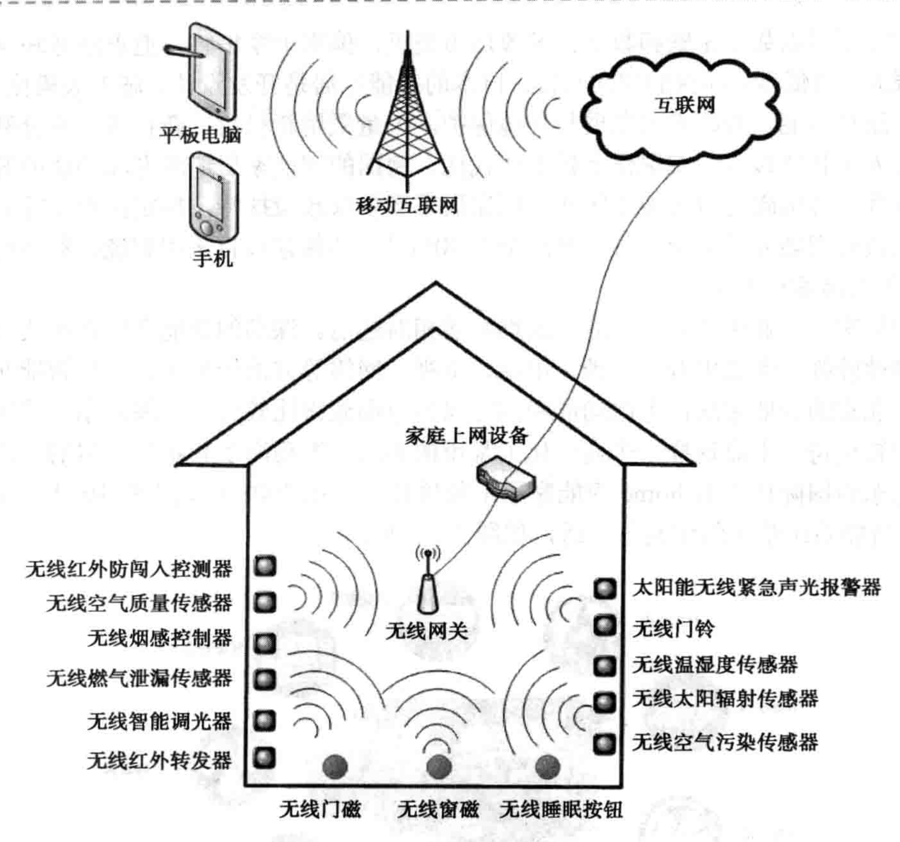


图 5-38　智能家居控制模型

（4）通过各种视频监控设备对家庭进行监控。

（5）通过 Internet 或者手机对家庭环境下的各种设备进行远程访问控制。

为了实现上述功能，可以将系统划分为智能灯光照明控制、智能家用电器控制、智能安全防范控制、智能监控、访问控制、智能家居网关六个子系统。

1. 智能灯光照明控制子系统

家庭内照明设备主要由荧光灯、吊灯、壁灯、射灯、落地灯和台灯等组成，除荧光灯外，其他所有灯均可作亮度调节，以满足不同的需要。智能灯光子系统由智能灯光控制面板组成，智能灯光控制面板与房间内照明设备对接后，即可实现强大的灯光场景效果，例如可以根据需要调节灯光强度，或对照明设备进行开关等。

2. 智能家用电器控制子系统

家用电器主要包括空调、热水器、电视机、电动窗帘等。智能家用电器控制子系统由智能电器控制面板组成，与房间内相应的设备对接后即可实现相应的控制功能，如设定热水器或者空调的温度、窗帘遮挡的范围等。



3. 智能安全防范控制子系统

智能安全防范子系统由各种智能探测器和智能网关组成，用于构建房间内的主动防御系统。智能红外探测器，探测人体的红外热量变化从而发出报警；智能烟雾探测器，探测出烟雾浓度超标后发出警报；智能门禁探测器，根据门的开关状态发出报警；智能燃气探测器，探测出燃气浓度超标后发出报警。该子系统可实现手机、电话、遥控器、计算机软件等方式接收报警信息，并能实现布防、撤防的设置。

4. 智能监控子系统

智能监控可以有效地了解家中的情况，如老人、小孩的状况。另外，实时录像功能对住宅起到了保护作用。

智能监控分为：

（1）室外监控，监控住宅附近的状况。

（2）室内监控，监控住宅内的状况。

（3）远程监控，通过手机、网络可随时查看监控区域内的情况。

智能监控子系统可实现实时查看、录像、录像调用、云台控制（即通过控制系统在远程控制摄像机等设备转动或移动）等功能。主要设备包括摄像机、视频服务器等。

5. 访问控制子系统

访问控制子系统包括智能遥控器、计算机综合管理软件、手机客户端软件等部分，实现对房间设备的综合访问管理和控制。

6. 智能家居网关子系统

智能家居网关在智能家居系统中有着举足轻重的作用。一方面，智能家居网关将家庭网络与外部网络连接，实现两者之间的信息交换；另一方面，智能家居网关自动收集各种在线设备的相关信息，生成设备描述文件，对各种设备进行集中控制和管理，是智能家居的核心。

智能家居依靠高科技实现了回归自然的环境氛围，促进了人文环境发展，依托先进的科学技术，实现家居管理的高效化、节能化和环保化，提高了人们的生活质量，促进可持续发展，是人类社会住宅发展的必然趋势。

5.6 物联网在智慧农业领域的应用

5.6.1 智慧农业现状和趋势

20世纪农业和农村经济与社会的发展也带来了农业用地减少、农田水土流失、土壤生产力下降、农产品与地下水污染以及生态环境恶化等问题。生态农业、绿色农业、智慧农业等先进的农业技术在这样的背景下产生。智慧农业是一种由信息、遥感技术与生物技术支持的定时、

定量实施耕作与管理的生产经营模式，它是现代信息技术与农业技术紧密结合的产物，是21世纪农业发展的重要方向。

智慧农业是农业生产的高级阶段，集新兴的互联网、移动互联网、云计算和物联网技术为一体，依托部署在农业生产现场的各种传感节点（环境温湿度、土壤水分、二氧化碳、图像等）和无线通信网络实现农业生产环境的智能感知、智能预警、智能决策、智能分析、专家在线指导，为农业生产提供精准化种植、可视化管理、智能化决策。

5.6.2 智慧农业典型应用

由于瓜果蔬菜对生长环境有着严格的要求，所以现代农业搭建了温室大棚（见图5-39）来控制植物的生长环境，以实现跨地区与跨季节的瓜果蔬菜培育。可见，环境在温室大棚中起着重要的作用。

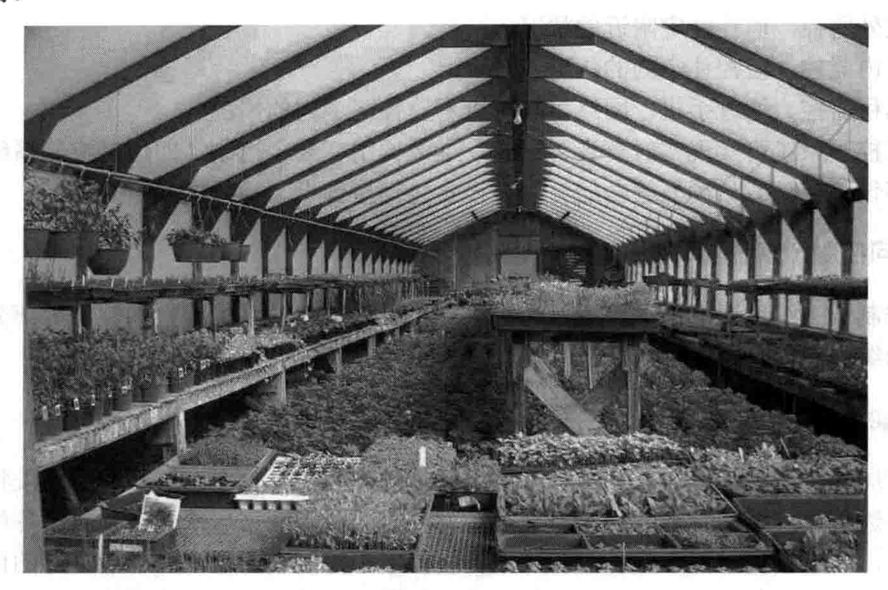


图5-39 温室大棚

传统的大棚环境控制，是通过全人工的方式来实现的。在每一大棚中放置一个温度计、湿度计、二氧化碳浓度计等，由技术员巡查每一个大棚的环境参数，若发现环境参数不对，就要采取一定的措施来进行补偿。比如，温度过高的话，就要打开卷帘通风或者打开通风机等。这样的操作方式对于只有少量大棚的农户，还可以应付得来，但如果大棚数量多，就需要花费大量的人工去查看各大棚的环境参数，对环境异常的大棚进行操作，大大降低了工作效率。

智能大棚（温室）自动控制系统，可对各不同大棚的环境参数进行实时的监测和报警，并可远程控制各大棚不同的电动设备，如卷帘机、灌溉机等。使技术人员在办公室就能对多个大棚的环境进行监测控制，以使植物获得最佳的生长环境，增加产量。

● 系统概述

智能大棚（温室）自动控制系统实现了对影响农作物生长的环境传感数据实时监测，同时



根据环境参数门限值设置实现自动化控制现场电气设备，如风扇、加湿器、除湿器、空调、照明设备、灌溉设备等，并支持远程控制。常用环境监测传感器包括：空气温度、空气湿度、环境光照、土壤湿度、土壤温度、土壤水分含量等传感器。亦可支持无缝扩展无线传感器节点，如大气压力、加速度、水位监测、一氧化碳、二氧化碳、可燃气体、烟雾、红外人体感应等传感器。智能大棚检测系统将互联网从桌面延伸到田野，让温室实时在线，从而实现蔬菜大棚与数据世界的融合。实时采集的传感器数据与传统的种植经验相结合，可以使农业专家随时远程查看农田内的各种数据（温度、湿度、光照、水量），判断是否是适合作物生长的最佳条件。专家根据自身经验以及对系统关键值的设定进行判别，当某种数据偏离设定值时，大棚会自动做出反应（温度偏低时则打开供暖设施，温度偏高时则开门通风，水量不足时则自动打开喷淋装置等）。该系统可同时监测和控制几十万座蔬菜大棚的正常运行，从而使农作物始终处在最佳的生长环境中。系统能够大幅度降低人工巡查的工作量，并对不安全状况提前进行预警，通过后台计算机轻松实现无人值守和远程监测。另外，还可以实现对蔬菜病虫害的早期预警和对蔬菜产量、交易价格的早期预测。通过更加精细和动态的监控方式对农作物进行管理，更好地感知农作物的生长环境。通过智能控制提高资源利用率和生产力水平，是充分发挥农业生产效率、减少农业资源浪费和农田污染的现代农业生产方式。

● 系统架构

农业生产环境是一个复合开放的生态系统，包含土壤、肥料、水分、光照、温度、空气、生物等因子，对农田环境数据进行快速、准确的采集、传输、控制，直接或间接对相关因素进行分析，有利于对农作物生产进行科学管理。

温室大棚自动控制系统采用物联网典型三层架构设计，如图 5-40 所示，用户可以像使用常用电气设备一样部署物联网系统，实现系统便携式、无线化、规模化。

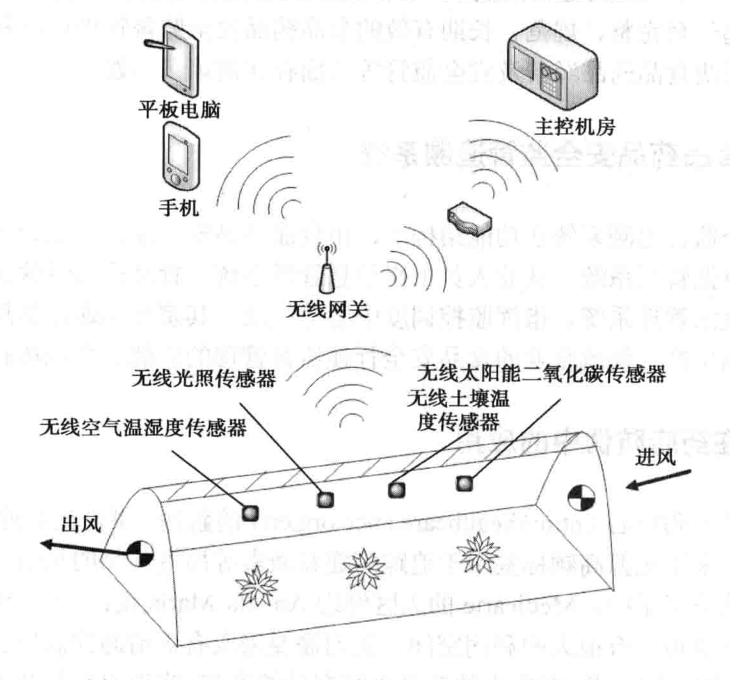


图 5-40　智能大棚检测系统三层架构



物联网感知层：该层的主要任务是将大范围内的现实世界农业生产等的各种物理量通过各种手段，实时并自动转化为虚拟世界可处理的数字化信息或者数据。

采集的信息主要有以下种类。

（1）传感信息：如大棚温度、湿度、压力、气体浓度、生命体征等。

（2）物品属性信息：大棚内物品名称、型号、特性、价格等。

（3）设备工作状态信息：如仪器、设备的工作参数等。

物联网传输层：该层的主要任务是将农业信息采集层采集到的传感器信息，通过各种网络技术进行汇总，将大范围内的传感器信息整合到一起，以供处理。传输层是物联网的神经中枢和大脑信息传递和处理的路径。网络层包括通信与互联网的融合网络、网络管理中心、信息中心和智能处理中心等。信息汇总层涉及的技术有有线网络、无线网络等。

物联网应用层：该层的主要任务是将信息汇总，并对汇总而来的信息进行分析和处理，从而对现实世界的实时情况形成数字化的认知和反馈。

5.7 物联网在食品药品追溯领域的应用

食品药品安全问题一直是百姓和社会最关注的问题之一。近年来，食品药品安全事故频发，给人民的身体健康和生命安全构成了严重威胁，同时也对社会经济和发展产生了重大影响。如何建立完善的食品药品安全监管体系，对食品药品进行有效的防伪、监控和追溯，已经成为我国迫切需要解决的课题。

物联网给贯彻国家有关食品药品安全的文件精神、解决监管过程中存在的问题提供了有力的技术支撑。基于物联网和其他相关技术，食品药品安全监管追溯平台成为可能：利用高科技、信息化手段建立起一套完整、规范、长期有效的食品药品安全监督管理体系和应急指挥调度系统，从而有效地解决食品药品经营及安全监管等方面存在的诸多问题。

5.7.1 物联网食品药品安全监管追溯系统

食品药品安全监管追溯系统在功能结构上，由食品药品安全监管追溯管理系统、食品药品经营和服务许可审批管理系统、从业人员上岗信息管理系统、食品药品经营企业台账远程巡查管理系统、移动执法管理系统、指挥监控调度中心等组成，其宗旨是通过信息化的手段使国家职能部门能对食品生产、物流企业的食品安全行使监督管理的职能。系统拓扑如图 5-41 所示。

5.7.2 物联网在药店防伪中的应用

根据中国物品编码中心（http://healthcare.ancc.org.cn）的新闻，哥伦比亚连锁药店 Medicarte 引进 RFID 技术，采用无源高频标签用于追踪癌症和激素等昂贵药物的包装，以防止废弃外包装落入制假等不法分子手中。Medicarte 的大区经理 Angela Maria 说：“治疗癌症和一些激素药物等非常昂贵，在黑市上有很大的利润空间，我们需要采取有效措施控制假冒产品的泛滥。通过运用 RFID 和生物识别技术，对售出的药品进行有效的追踪，实现对空包装的最大限度收回。”



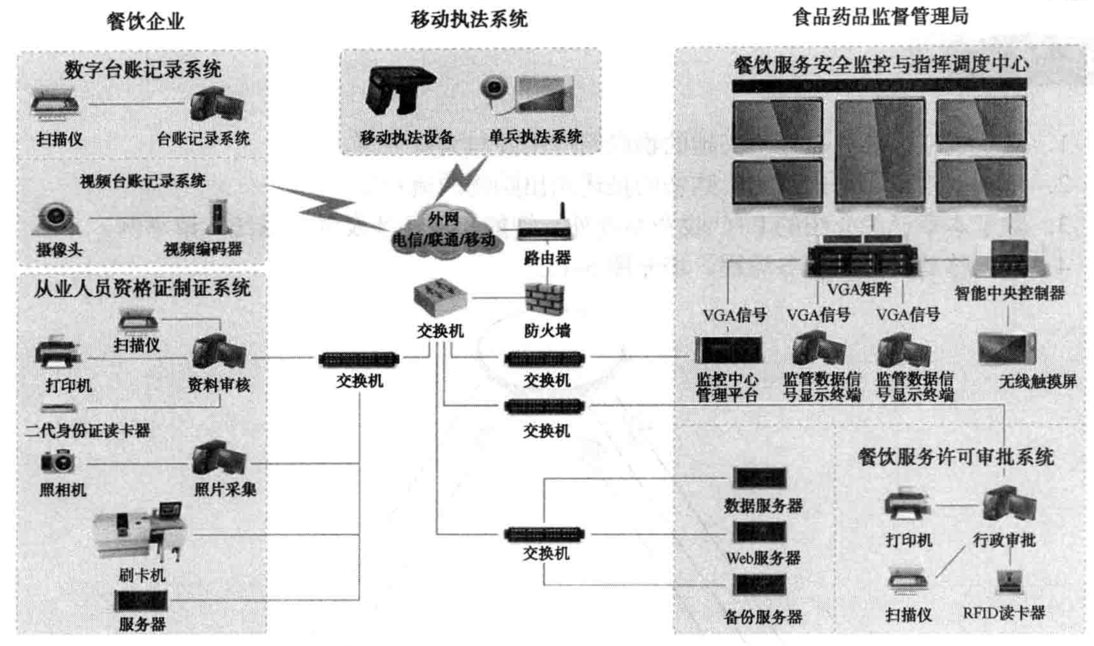


图 5-41　食品药品安全监管追溯系统拓扑图

哥伦比亚麦德林地区的RFID解决方案提供商IDlink负责该系统的开发。Medicarte将Tagsys符合ISO 15693 标准的RFID无源高频（HF）标签粘贴到药品的外包装上。Tagsys LP-101读写器读取标签中存储的预编码的序列号，该信息通过Aero LC天线发出。Medicarte员工将该批次药品的类型、有效期等信息输入软件数据库。

顾客第一次到药店买药时，系统将存储其指纹信息。药剂师使用HID Global的OMNIKEY 5321 USB RFID读写器读取药包装上的标签，将标签的序列号与顾客建立联系。

药店规定，患者再次买药时应将已用过的药品包装返回药店。公司声明，这在法律上并没有强制执行，这主要是为了减少市面上假冒伪劣产品的横行。

病人将手指放到指纹识别器上，识别数据与已经记录的数据相匹配，查看是否已经购买过此类药品。使用Omnikey读写器读取包装上的标签数据，确保该客户与药品的相匹配性。

该解决方案助力 Medicarte 公司追踪贴标签药品的总数量，并监测实际发到病人手中的数量。另外还有助于监控药品的保质期。药店出售即将过期的药品时，店内的计算机会及时发出警报。 该系统目前已在波哥大、卡利、麦德林、巴兰基亚、佩雷拉和马尼萨莱斯城投入使用。该基于云的管理软件与Medicarte企业资源计划（ERP）软件集成。部署RFID系统之前，病人购买的药品信息都是通过手工记录的。RFID技术大大降低了手工记录可能引起的出错率。

RFID技术大大简化了公司内部流程，有望将系统扩展到供应链源头。2012年，Medicarte计划将手机NFC技术应用到药品送货上门的服务中。配送人员在顾客家门口用手机扫描包装上的标签信息，并将标签编码发送到公司ERP系统，通过GPS坐标，确保送货的准确性。

5.8 练习题

1. 查找资料，寻找自己感兴趣的物联网应用并与大家分享。
2. 请根据本章“未来商店”购物的描述画出购物的流程图。
3. 除了本章已经介绍的 ETC 收费系统外，智能交通还涉及哪些系统？请举例。
4. 根据移动支付的业务流程，填充图 5-42。

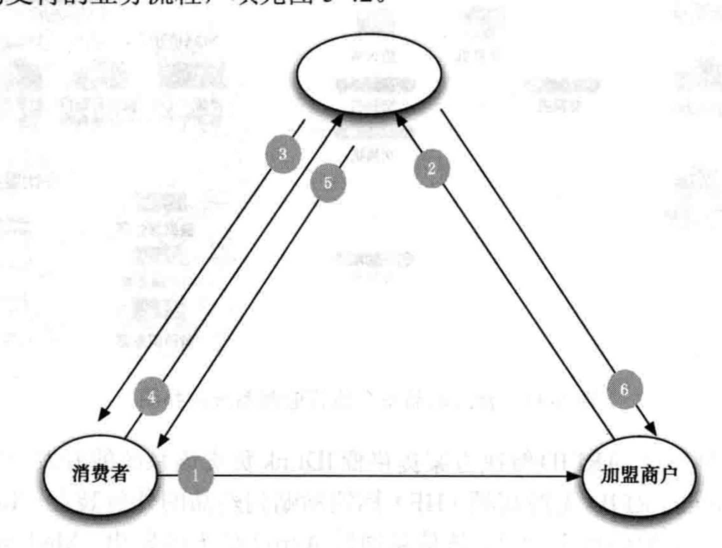


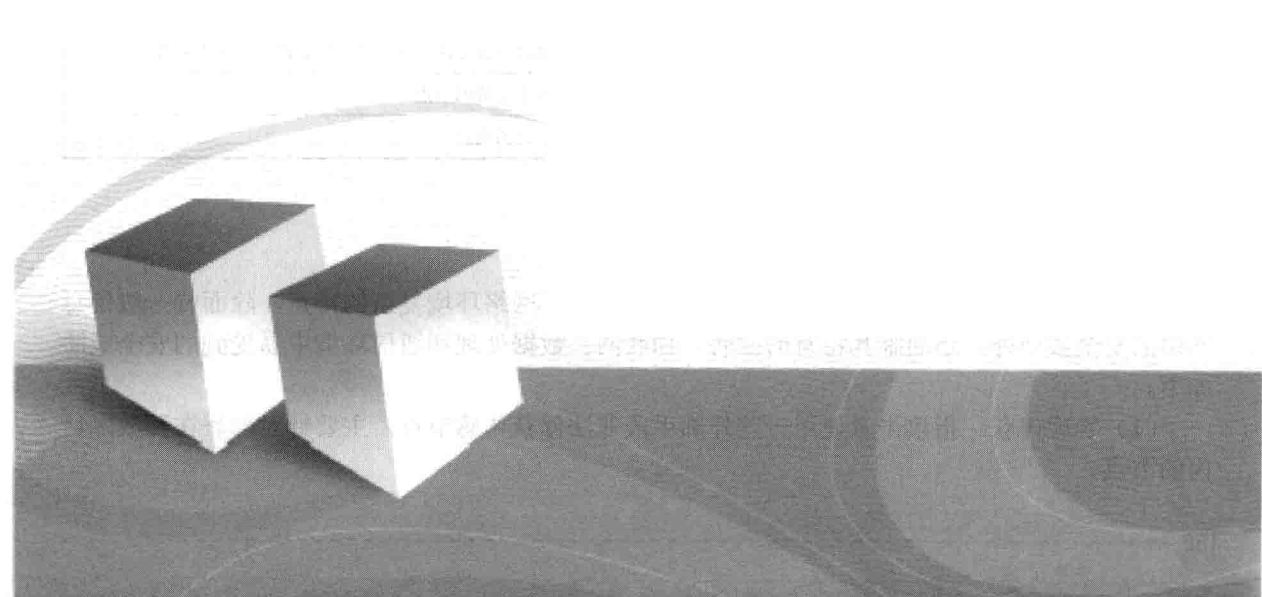
图 5-42　移动支付流程

5. 智能家居有哪些关键技术？请列举一些国内外的智能家居系统。

第6章

物联网工程安全

物联网建立在互联网的基础之上，将人们和身边无数物品联系起来，它的安全性除包括传统互联网安全要求外，还有其自身的安全要求，如感知层的安全性和应用层的安全性。考虑到高职学生的特点，本章重点分析物联网安全特征与目标，着重介绍物联网在感知层和网络传输层的安全问题。



6.1 物联网工程安全目标

6.1.1 安全目标

物联网应用系统中的数据大多是一些应用场景的实时数据，其中不乏国家、城市重要行业、公司、部门甚至个人敏感数据，物联网应用系统的安全保证是物联网健康发展的重要保障。

信息与网络安全的目标是要保证被保护信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。这个要求贯穿了物联网的感知信息采集、汇集、融合、传输、决策等信息处理的全过程，所面临的安全问题包括但又不同于现有网络系统的特征。

首先，在感知数据采集、传输与信息安全方面，感知节点通常结构简单、资源受限，无法支持复杂的安全功能；感知节点及感知网络种类繁多，采用的通信技术多样，相关的标准规范不完善，尚未建立统一的安全体系。

其次，在物联网业务的安全方面，支撑物联网业务的平台具有不同的安全策略，大规模、多平台、多业务类型使得物联网业务层次的安全面临新的挑战；另一方面，从信息的机密性、完整性和可用性角度分析物联网的安全需求和特征。物联网信息机密性直接体现为信息隐私，如感知终端的位置信息。在数据处理过程中同样也存在隐私保护问题，要建立访问控制机制，控制物联网中信息采集、传输、查询等操作。

总之，物联网的安全特征体现了感知信息的多样性、网络环境的复杂性和应用需求的多样性，给安全研究提出了新的更大的挑战。物联网以数据为中心的特点和应用密切相关性，决定了物联网总体安全目标（见表 6-1）。

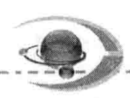
表 6-1 物联网总体安全目标

目　标	内容描述
可用性	确保感知网络的信息和服务在任何时间都可能提供给合法用户
机密性	避免非法用户读取机密数据，一个感知网络不应泄露数据到相邻网络
完整性	通过校验来检测数据是否被篡改。数据完整性是确保消息被非法（未经认证的）改变后才能够被识别
不可否认性	避免物联网节点被恶意注入虚假信息，确保信息来源于正确的节点
时效性	保证接收到数据的时效性，确保没有恶意节点重放过时的消息

6.1.2 安全威胁

物联网具有感知层网络资源受限、拓扑变化频繁、网络环境复杂的特点，除面临一般信息网络的安全威胁外，还面临其特有的威胁。物联网在数据处理和通信环境中易受到的安全威胁如下。

（1）物理俘获。指攻击者使用一些外部手段非法俘获传感节点，主要针对部署在开放区域内的节点。



（2）传输威胁。物联网信息传输主要面临中断、拦截、篡改、伪造等威胁。

（3）自私性威胁。网络节点表现出自私、贪心的行为，为节省自身能量拒绝提供转发数据包的服务。

（4）拒绝服务威胁。指破坏网络的可用性，降低网络或系统执行某一期望功能的能力，如硬件失败、软件瑕疵、资源耗尽、环境条件恶劣等。

6.1.3　安全体系

根据物联网的安全威胁和特征，物联网的安全体系包括以下 3 个部分。

1. 基于数据的安全

该部分主要处理数据的保密性、鉴别、完整性和时效性。用于保障数据安全的方法主要包括以下两点。

（1）安全定位。物联网应具有在存在恶意攻击的条件下，仍能有效、安全地确定节点的位置的能力。

（2）安全数据融合。物联网应在任何情况下保证融合数据的真实性和准确性。

2. 基于网络的安全

网络通信为应用服务层提供数据服务，在考虑网络安全问题时应基于以下安全策略。

（1）安全路由。防止因误用或滥用路由协议而导致的网络瘫痪或信息泄露。

（2）容侵容错。网络传输层安全技术应避免故障、入侵或者攻击对系统可用性造成的影响。

（3）基于网络的安全还应该使用网络可扩展策略、负载均衡策略和能量高效策略等。

3. 基于节点的安全

基于节点的安全为网络传输层通信和应用服务层数据提供安全基础设施，可采用以下安全机制。

（1）安全有效的密钥管理机制。

（2）高效冗余的密码算法。

（3）轻量级的安全协议。

6.2　RFID 系统安全

作为物联网感知层重要设备之一的 RFID 技术因其具有防水、读取距离远、读取速度快、存储容量大且数据可加密、抗污染能力和耐久性、可重复使用等优点，已被广泛应用于交通、物流、医疗、食品安全、零售、制造、海关、安检、机场等应用领域，可见，RFID 系统安全直接关系到物联网安全和应用的推广。另外标签信息泄露，如护照、身份证、处方等都会侵犯个人隐私，因此 RFID 系统的安全一直是研究的热点问题之一。

一般情况下，阅读器和后台数据库之间的通信可以认为是安全可靠的。关键是标签、读

写器安全，因此，我们把 RFID 系统安全问题主要分为：物理安全、通信安全、信息安全三个方面。

6.2.1 RFID 物理安全

1. 读写器伪造

RFID 读写器伪造是 RFID 系统面临的一大威胁。RFID 读写器与主机之间的通信可以采用传统的攻击方法截获，RFID 读写器自然也是攻击者要攻击的对象。

2. 电子标签伪造

电子标签伪造是 RFID 系统面临的另一大威胁。如果不法分子能够轻易地伪造电子标签就意味着能够篡改商品或人员的身份，轻而易举地破坏 RFID 系统的信用。比如在 RFID 的商品防伪应用领域，能够非法伪造 RFID 意味着防伪系统的失败，目前防止伪造的主要对策是通过 ID 加密、特殊加工等方法提高伪造的成本。另外，为防止 RFID 的重复利用，采用特殊工艺把 RFID牢固地固定在物品的开启之处，一旦物品开启标签就损坏，不能再利用。比如酒的防伪应用中，RFID 内嵌在木塞里，只要开启木塞，里面的 RFID 就遭破坏，无法再利用。

3. RFID 碰撞

随着 RFID 技术的应用越来越广泛，很多时候不可避免地会出现多个标签进入识别区域，使得信号互相干扰，RFID 技术存在的问题也越发突出，其中 RFID 冲突问题就是其中之一。

目前，多读写器对标签的干扰问题主要由标签自身的抗干扰能力来解决。对读写器碰撞问题，人们首先考虑在工程安装时按读写器可识读范围不重叠的原则来安装，但因 RFID 读写器具有很高的灵敏度，它甚至可以接收空间里的 1 个纳瓦的能量，因此读写范围不重叠的相距较远的读写器之间也会发生读写器碰撞的问题。目前，针对多读写器碰撞的解决方法有时隙分配、信道分配、载波侦听、功率控制等方法。

6.2.2 RFID 通信安全

RFID 使用的是无线通信信道，这就给非法用户的攻击带来了方便。攻击者可以非法截取通信数据；可以通过发射干扰信号来堵塞通信链路，使得读写器过载，无法接收正常的标签数据，制造 DoS 攻击；可以冒名顶替向 RFID 发送数据，篡改或伪造数据。笔者归纳出以下几种方法供针对性地改进。

1. Hash 函数

因为 RFID 标签芯片计算资源有限，利用 Hash 函数技术实现了防止消息泄露、伪装、定位跟踪等安全攻击。



2. 可靠安全机制

为 RFID 系统构造一个可靠的安全机制用于 tag 与 reader 间的相互认证和传输数据。所有的安全机制都需要建立在一个加密算法的基础之上。但由于 RFID 标签的使用数量大、范围广，必须将其造价控制在比较低廉的水平，这使得 RFID 标签通常只能拥有 5000～10 000 个逻辑门，而这些逻辑门主要用于实现一些最基本的标签功能，仅剩少许可用于实现安全功能。但实现 AES（advanced encryption standard）算法需要 20 000～30 000 个逻辑门，实现 RSA、椭圆曲线密码等公钥密码算法则需要更多的逻辑门。因此，大多数 RFID 标签根本无法提供足够的资源来实现一些比较成熟和先进的加密算法，而只能采用一些“PIN 码”或“password”机制来保护秘密数据。

3. 调低读写器功率

读写器的输出功率要远远大于无源电子标签，因此读写器的电波传送距离要比无源电子标签远得多，比如超高频的读写器和无源电子标签的最大通信距离大约是 5 米，这主要是受电子标签的功率和天线尺寸的限制，而读写器本身的电波可以传播到很远的地方。如果有人在离读写器较远的地方架设天线，截取读写器的电波信号，就很难被人察觉。通过截收读写器发射的电波来获取信息是一件非常专业的工作，需要非常大的成本投入，一般的 RFID 系统并没有必要考虑这种信息泄露风险，但对一些机密性非常大的信息需要考虑防范措施，比如用吸波材料封闭读写器作业空间，适当调小读写器的输出功率。

4. 认证协议

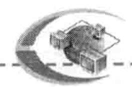
RFID 系统的 Gen2 类标签容量有限，仅支持单片 16 bit 伪随机数发生器（PRNG）和用于数据传输过程中探测错误的循环冗余码（CRC）校验的特点，难以实现复杂的安全算法。因此，有人提出基于异或运算的方法，将标签 32 位 ID 号分为低 16 位和高 16 位，利用标签的 CRC-16 位生成相应校验码作为密文传输。该协议解决了已有协议在信息保密性、不可跟踪性、前向安全性、Tag 反克隆性、不可重放性 5 个方面安全性的问题，提高了数据库查询速度，降低了 RFID 标签的设计成本。

6.2.3 RFID信息安全

信息泄露是指暴露标签发送信息，这个信息包括标签用户或识别对象的相关信息。如 RFID 设备管理信息是公开的，但当电子标签应用于药品时，很可能暴露药物使用者的病理。当个人信息如电子档案、生物特征添加到电子标签中时，标签信息泄露问题便极大地危害了个人隐私。美国于 2005 年 8 月在入境护照装备电子标签的计划，因考虑到信息泄露的安全问题已经被推迟。RFID 信息安全表现在以下几个方面。

1. 恶意追踪

因为 RFID 系统后端服务器提供数据库，所以标签不用包含和传输大量的信息。通常只需



传输简单的标识符，人们可以通过这个标识符访问数据库，获得目标对象的相关数据和信息。可以通过标签固定的标识符追踪它，即使标签进行加密后不知道标签的内容仍能通过固定的加密信息追踪标签。换言之，可以在不同的时间和不同的地点识别标签，得出标签的定位信息。一旦标签的定位信息暴露也就意味着标签可以长期地被追踪。因此，可以通过标签的定位信息获得标签持有者的行踪。

虽然视频监视、GSM、蓝牙等技术也允许追踪，但是标签识别装备相对价格低廉，特别是RFID进入百姓生活后，拥有阅读器的人都可以扫描并追踪别人。而且被动标签信号不能切断，尺寸很小，极易隐藏并且使用寿命很长，可以自动化地识别和采集数据，这就加剧了恶意追踪的问题。RFID系统中最主要的安全风险是“数据保密性”。显然，没有安全机制的RFID标签会向邻近的识读器泄露标签内容和一些敏感信息。由于缺乏支持点对点加密和PKI密钥交换的功能，在RFID系统应用过程中，攻击者有许多机会可以获取RFID标签上的数据。RFID系统中的另一个安全风险是“位置保密性”。如同个人携带物品的商标可能泄露个人身份一样，个人携带物品的RFID标签也可能会泄露个人身份，通过识读器就能跟踪携带不安全RFID标签的个人。

2. 窃取电子标签数据

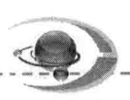
电子标签可能含有企业关键信息或个人隐私信息，比如产品的生产批次、生产数量、个人身份、购物习惯等，如果这些电子标签被盗，意味着企业内部信息或个人隐私信息被泄露。为了防止数据的被窃，可采用以下两种方法：①数据加密；②电子标签不存敏感数据，只存无特殊意义的ID信息，关键数据分散在各个服务器中。

3. 篡改电子标签数据

如果巧妙地篡改电子标签的数据，可能造成非法物品或数据容易混入整体业务系统，最终破坏业务的运行。防止数据被篡改的主要方法有：①限制存储器的写入次数。如果标签在业务整体流程中数据不需要改变，就可以采用只读标签或一次性读写标签。切断了篡改数据的物理手段。②限制存储器的可写区域。提前把存储器的区域分割成可写区域和不可写区域，把关键数据（如标签ID）放进不可写区域，可以防止关键数据被篡改。③密码保护。预先设定密码来保护数据，每个标签的密码不一样，需要增加密码管理成本。④变更存储器区域读写属性。对关键数据区域或全体区域设置只读属性就可以防止篡改。四个措施可以根据成本要求单独使用，也可以复合使用。

4. 往电子标签植入病毒

电子标签由于存储量很小，且存储的是数据而不是执行代码，很难把病毒本身写进标签本体中，但是篡改存储器中的参数变量（比如数据长度等）扰乱系统处理的可能性大，如果在中间件、服务器软件方面进行严格的排错处理，可以保证系统的正常运行。目前还没有有关电子标签内植入病毒，引起系统崩溃的实际案例的报道，成品电子标签也没有防病毒的措施，但随着电子标签的大容量、高智能化的发展，今后需要研究病毒的寄生机制和防范措施。



5. 泄露电子标签数据格式

电子标签数据格式需要对外保密，如果这些数据被泄露，不法分子就很容易进行标签的伪造和篡改。有些重要的数据要进行分散管理，即不能把所有数据集中到一个人身上，以防一旦此人出事，所有的数据暴露无遗。要对标签的制作进行严格的管理，比如设门禁系统，安装计算机操作记录追查系统等。

6.3 无线传感器网络安全

无线传感器网络具有部署环境恶劣、网络规模庞大、节点数目众多等特性，使得截取、窃听和伪造信息比传统网络更加容易。图 6-1 为无线传感器网络结构，无线传感器网络安全问题影响了它的应用。另外，网络拓扑结构的变化、路由信息的交换、最佳路由的选择、目的节点的定位、产生和维护以及数据的转发等操作都是由相应的路由协议来完成的。因此，无线传感器网络安全问题主要体现在物理层（PHY）安全、链路层（MAC）安全、路由安全等多方面。

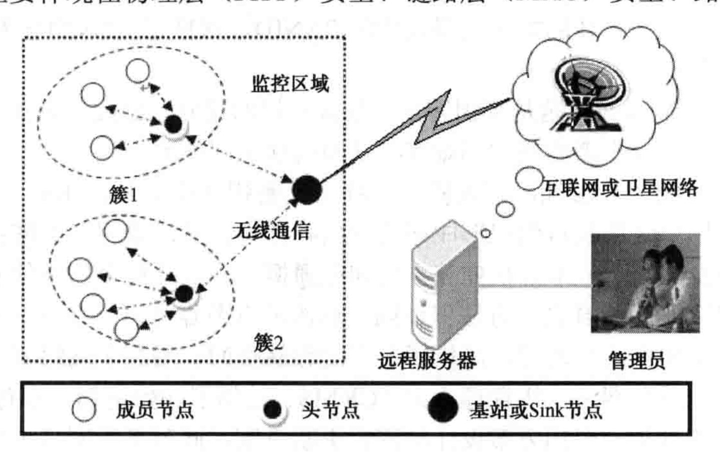


图 6-1 无线传感器网络结构

1. 物理层的安全威胁

由于 WSN 的特点，攻击者可以很容易地对单个甚至多个通信链路间传输的信息进行窃听，并从多个传感信息中分析出敏感数据。同时，通过传感信息包的窃听，还可以对 WSN 中的网络流量进行分析，从而分析出传感节点的位置。一旦定位到传感节点，攻击者就可以捕获传感器节点，并通过捕获到的节点获取重要的信息（如密钥），也可以将捕获的节点进行修改后重新放入 WSN 中，进行更为隐蔽的攻击和破坏。另外物理层安全威胁的另一种方式是电波干扰，攻击者通过在 WSN 中随机放入少量的干扰节点使整个网络瘫痪。

2. 链路层的安全威胁

链路层的安全威胁来自于数据包破坏，攻击者通过破坏数据包中一个字节，使得接收方无法正确校验，从而产生失败的 ACK。而对于多数的 MAC 协议，失败的 ACK 将导致指数级增

长的重传，从而降低 MAC 的传输效率。

3. 路由安全威胁

（1）PANID 的机密性。

当前 ZigBee 网络的计数模式加密或密码块链消息认证码安全措施注重于应用数据的安全保证。然而，这并不代表能够保证整个 ZigBee 网络的安全。由于安全方案大多数针对 MAC 层载荷（应用数据），而没有对 MAC 帧头信息进行必要的保护，使得无线传感网与互联网类似，也存在很多的攻击。

ZigBee 协议的连接请求或连接回应都是以 MAC 帧为载体。并且在传输过程中，MAC 帧头信息都是以明文形式传输的。这就会使攻击者通过 Sniffer 等专业工具获取目的 PANID 和源 PANID；进而可以根据所获得 PANID 伪装成合法协调器，与网络其他设备进行通信。

考虑到因MAC层帧头信息没有实施必要的保护使得攻击者能够获得目的PANID等相关机密信息，为此可在 MAC 层中添加一个模块：以帧的序列号为初始向量，采用 AES 算法对相应的 PANID 进行加解密，对 PANID 进行合理保护，保证每次发送的 MAC 帧的 PANID 不同，使得攻击者无法借助数理统计的方法获得真实的 PANID，保证了 PANID 的机密性。

（2）密钥静态管理。

ZigBee 网络安全最大的问题是密钥管理，包含密钥的建立、分发、更新等环节。有效的密钥管理可以显著地增加攻击者的成本和难度，从而确保了网络安全。

为了提高密钥分配抗攻击性，有人提出一种三元密钥（Kc、Kn、Ks）分配算法：首先根据 LEACH 协议采用单级簇头自组织形成网络的拓扑结构，然后采用三类密钥的方式进行密钥预分配，提高网络抗攻击性、节点抗捕获能力和连通概率，保证整个网络的安全通信。还有人提出 WSNKG 方案，采用组合设计方法保证同一簇内所有节点可直接建立共享密钥，而不同簇的节点可通过基站构建多路径密钥，降低了节点的存储空间，增强了网络安全性和抗毁性。

基于簇的无线传感器网络密钥管理方案（CKMS）包括了初始密钥、专有密钥、扩充密钥、对偶密钥和簇密钥 5 种类型密钥方案设计与密钥更新机制，同时支持网络扩展，具有较小的通信开销和计算开销，占用较少的存储空间并且连通性好。

考虑到传统密钥管理方案使传感器节点之间共享密钥，传感器节点之间出现能量消耗不均衡现象，引起整个网络安全性降低，因此能量均衡的网络密钥分配方案是一个不错的想法：根据传感器节点的能量建立源和目的传感节点间多条不相交路径，根据传感器能量最小和最大原理，为源和目的传感器节点之间建立一条最优传感器节点不相交路径，作为协商路径密钥的通道。

（3）密钥动态管理。

2006 年，Eltoweissy 在 Exclusion Basis Systems 和传感器网络的分簇结构基础上提出了动态密钥管理的概念，与静态密钥管理相比，主要优点表现在：①网络规模不受节点存储空间限制，适合于大规模分簇式网络；②可以动态而且高效地取消任意节点所拥有的全部密钥，从而驱逐被敌人捕获的节点，提高了网络的安全性能；③在提供同等安全性保证的条件下，相比于静态密钥管理，既节约了存储空间，又提高了能量效率。

适合于大规模分簇式无线传感器网络的动态密钥管理方法——EEHS，它具有安全性强、能量效率高、动态性能好、可扩展性强等特点，显著地提高了网络的抗捕获能力。当节点被捕



获时，EEHS 还可以动态取消并更新被捕获节点所拥有的全部密钥，最终驱逐被捕获的节点。为提高网络的能量效率和鲁棒性，EEHS 将密钥分配和密钥生成等功能分配给簇内不同的功能节点，且传感器节点轮流作为功能节点使用。

将 Blom 的密钥预分配方案和传感器网络部署后的地理信息相结合，并运用矩阵理论可实现密钥预分配、传感器节点部署、密钥直接建立和密钥间接建立 4 个阶段，并可提供当新节点加入或旧节点离开时的密钥管理方法。

4. 安全路由的设计目标

无线传感器网络安全隐患在于：网络拓扑部署区域的开放特征和无线网络的广播特征（即时空暴露）、信息极易窃取和篡改、缺乏有效的安全路由协议的设计等。无线传感器网络路由协议分为以数据为中心的路由协议、层簇式路由协议、基于地理位置的路由协议和能量感知的路由协议四大类，遇到常见攻击类型如表 6-2 所示。

表 6-2　路由协议及易攻击类型

协议类型	路由协议	攻击类型
以数据为中心的路由协议	Flooding, Gossiping, Directed diffusion, Rumor routing	Hello 包洪泛攻击、路由欺骗攻击、选择性转发攻击、女巫攻击、槽洞攻击、虫洞攻击等
层簇式路由协议	LEACH，TEEN，SOP，PEGASIS	路由欺骗攻击、选择性转发攻击、女巫攻击、槽洞攻击、虫洞攻击等
基于地理位置的路由协议	GEAR，GPSR，TBF	路由欺骗攻击、选择性转发攻击、女巫攻击等
能量感知的路由协议	SPAN，GAF，CEC，AFECA	Hello 包洪泛攻击、路由欺骗攻击、女巫攻击

尽管无线传感器网络的工作环境和工作任务不同，其安全目标和安全设计策略也不同，但其有两个共性：①共性的安全路由协议设计。例如冗余、MAC、散列、入侵检测、入侵容忍、网络自愈和重构、信息的加密和解密、数字签名、身份认证和访问控制等；②共性的安全评价机制。例如从可用性、机密性、完整性、不可否认性和时效性 5 个方面来进行评价。无线传感器网络安全路由的设计目标以及实现该目标的主要技术如表 6-3 所示。

表 6-3　安全目标实现技术

设计目标	设计要求	实现技术
可用性	在网络受到常规或非致命攻击（如 DoS）情况下，网络能够正常服务	冗余、入侵检测、入侵容忍、网络自我修复、网络重建
机密性	保证只有授权的用户才能够接收和发送合理的信息	信息加密、信息解密
完整性	保证信息不被篡改	哈希函数、MAC 捆绑、数字签名
不可否认性	保证发送者不能抵赖自己发送的信息	授权认证、数字签名、访问控制
时效性	保证接收到节点信息在生存周期内	入侵检测、访问控制

6.4 物联网传输层的安全

1. IPSec

IPSec（IP Security）是一个开放式的 IP 网络安全标准，它在 TCP 协议栈中间位置的网络层实现，可为上层协议无缝地提供安全保障，高层的应用协议可以透明地使用这些安全服务，而不必设计自己的安全机制。

IPSec 提供 3 种不同的形式保护 IP 网络的数据。

- 原发方鉴别。可以确定声称的发送者是真实的发送者，而不是伪装的。
- 数据完整性。可以确定所接收的数据与所发送的数据是一致的，保证数据从原发地到目的地的传输过程中，没有任何不可检测的数据丢失与改变。
- 机密性。使相应的接收者能获取发送数据的真实内容，而非授权的接收者无法获知数据的真正内容。

IPSec 通过 3 个基本的协议来实现上述 3 种保护，它们是鉴别报头（AH）协议、封装安全载荷（ESP）协议、密钥管理与交换（IKE）协议。IPSec 的体系架构如图 6-2 所示。

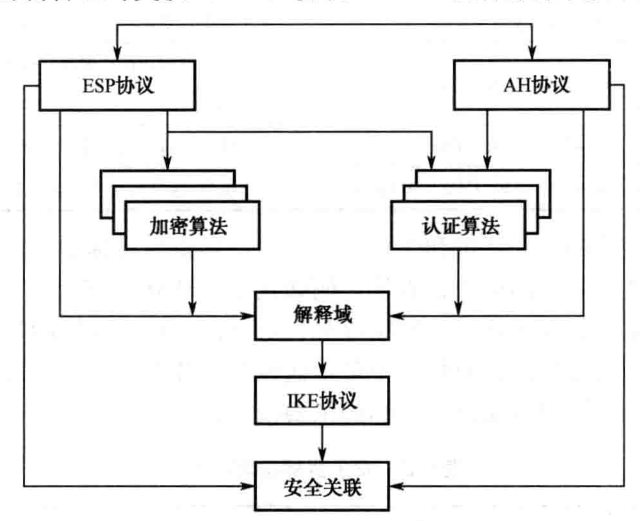
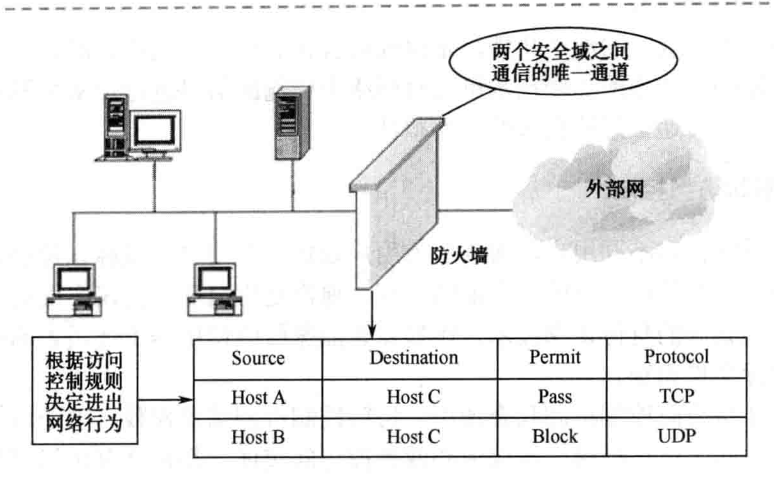


图 6-2　IPSec 的体系架构

2. 防火墙

防火墙是部署在两个网络系统之间的一个或一组部件（硬件设备或软件），这类组件定义了一系列预先设定的安全策略，要求所有进出内部网络的数据流都通过它，并根据安全策略进行检查，只有符合安全策略，被授权的数据流才可以通过，由此保护内容网络的安全。值得注意的是，防火墙在逻辑上进行隔离，而不是物理上的隔离，如图 6-3 所示。





Source	Destination	Permit	Protocol
Host A	Host C	Pass	TCP
Host B	Host C	Block	UDP

图 6-3　典型的防火墙体系结构

3. 隧道服务

物联网应用系统中有时候会使用一些自己建立的内部网络（Intranet），这类内部网络也必须通过互联网进行互联。这类服务往往是通过隧道技术提供的，最典型的就是虚拟专网（Virtual Private Network，VPN）。VPN 是指通过在一个公用网络（如互联网）中建立一条安全、专用的虚拟隧道，连接各地的不同物理网络，从而构成逻辑上的虚拟子网。进入 VPN 专用网络的各个终端，无论物联网络位置是哪里，使用上还是类似于同一个局域网进行操作。

隧道技术主要应用于 OSI 的数据链路层和网络层。数据链路层协议主要是将需要传输的协议封装到 PPP 中，把新生成的 PPP 报文封装到隧道协议包中，利用数据链路层协议进行传输。数据链路层隧道协议主要是 L2TP。网络层协议主要是把传输的协议包直接封装到隧道协议包中，再通过网络层进行传输，如图 6-4 所示。网络层隧道协议主要有 IPSec、IPv6、IPv4 等。

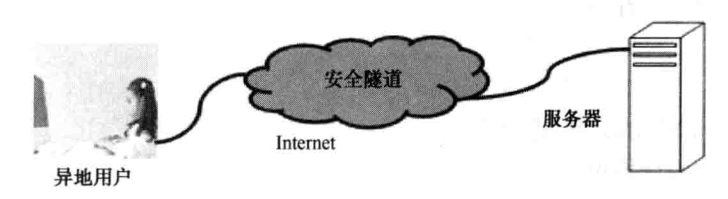


图 6-4　用安全隧道连接客户端和服务器

4. 数据签名与数字证书

数字签名包括两个过程：签名者对给定的数据单元进行签名；接收者验证签名。

签名过程需要使用签名者的私有信息（满足机密性和唯一性），验证过程应当仅使用公开的规程和公开的信息，这些公开的信息不能计算出签名者的私有信息。数字签名算法与公钥加密算法类似，是私有密钥或公开密钥控制下的数学变换，而且通常可以从公钥加密算法派生而来。

数字证书是一种权威性的电子文档，是由权威公正的第三方机构，即证书授证中心签发的证书。它以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验收，确保网上传递信息的机密性、完整性。

5. 身份识别和访问控制

物联网应用系统针对不同用户，通常会为用户设定一个用户名或标识符的索引值。身份识别是后续交互中用户对其标识符的一个证明过程，通常是由交互式协议实现的。一些物联网应用系统会采用一些新兴的身份识别技术，比如在智能家居中使用基于使用者的指纹、面容、虹膜等生物特征进行身份识别。

身份识别往往与访问控制机制联合使用。访问控制机制确定权限，授予访问权。实体如果试图进行非授权访问，将被拒绝。授权中心或者被访问实体，都建立有访问控制列表，记录了访问规则。

此外，还可以为访问的实体和被访问的实体划分相应的安全等级和范围，制定访问交互中双方的安全等级、范围必须满足的条件。

6.5 实训

6.5.1 实训一：简易防火墙配置

1. 任务目标

（1）了解 Windows 防火墙。
（2）了解简易防火墙的配置。
（3）掌握安全规则的建立。

2. 设备准备

（1）带 Windows XP 的计算机一台。
（2）能正常运行的局域网。

3. 任务实施

（1）Windows 防火墙的应用。

① 启用 Windows 防火墙。

步骤 1：选择“开始”→“设置”→“控制面板”命令，打开“控制面板”界面，双击其中的“Windows 防火墙”图标，打开“Windows 防火墙”对话框，如图 6-5 和图 6-6 所示。





图 6-5 “控制面板”界面

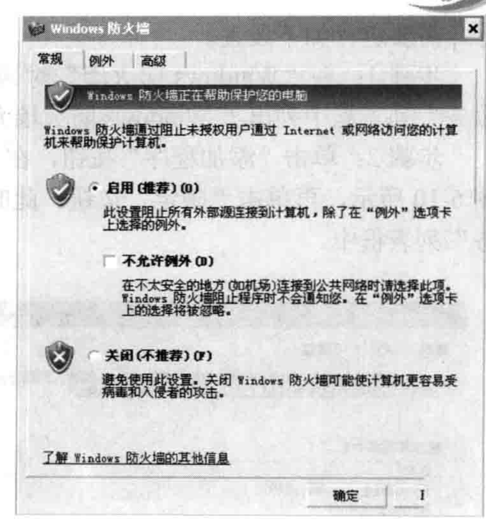


图 6-6 “Windows 防火墙”对话框

步骤 2：在“常规”选项卡中，选中“启用（推荐）”单选按钮。

② 设置 Windows 防火墙允许 ping 命令运行。在默认情况下，Windows 防火墙是不允许 ping 操作的，即当本地计算机开启 Windows 防火墙时，在网络中的其他计算机向本地计算机运行 ping 命令、发送数据包时，本地计算机将不会应答，其他计算机上会出现 ping 命令的超时错误。如果要让 Windows 防火墙允许 ping 操作，需要进行如下设置。

步骤 1：在“Windows 防火墙”对话框中选择“高级”选项卡，如图 6-7 所示。

步骤 2：单击 ICMP 选项组中的“设置”按钮，打开“ICMP 设置”对话框，选中“允许传入回显请求”复选框，如图 6-8 所示，再单击“确定”按钮。

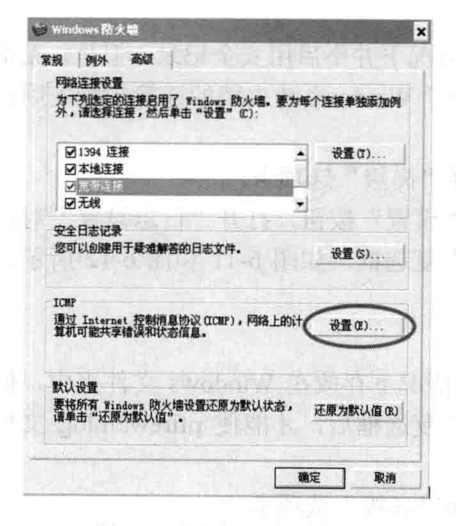


图 6-7 “高级”选项卡

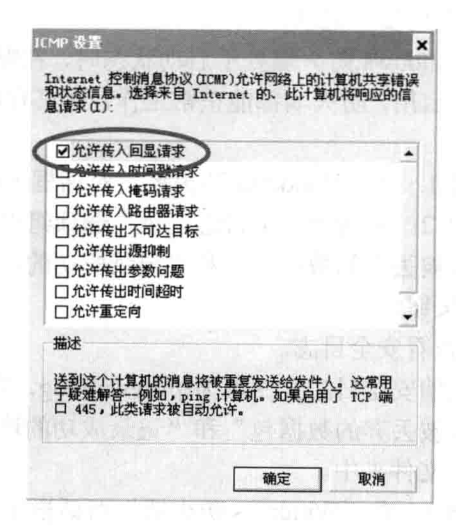


图 6-8 “ICMP 设置”对话框

③ 设置 Windows 允许 QQ 程序运行。

在默认情况下，Windows 防火墙将阻止 QQ 程序运行，如果要让 Windows 允许 QQ 程序运

行，需要进行如下设置。

步骤 1：在“Windows 防火墙”对话框中，选择“例外”选项卡（见图 6-9），在“程序和服务”列表框中列出了 Windows 防火墙允许进行传入网络连接的程序和服务。

步骤 2：单击“添加程序”按钮，在“添加程序”对话框中选中“腾讯 QQ2011”程序，如图 6-10 所示，再单击“确定”按钮。此时，QQ 程序就添加到“例外”选项卡中的“程序和服务”列表框中。

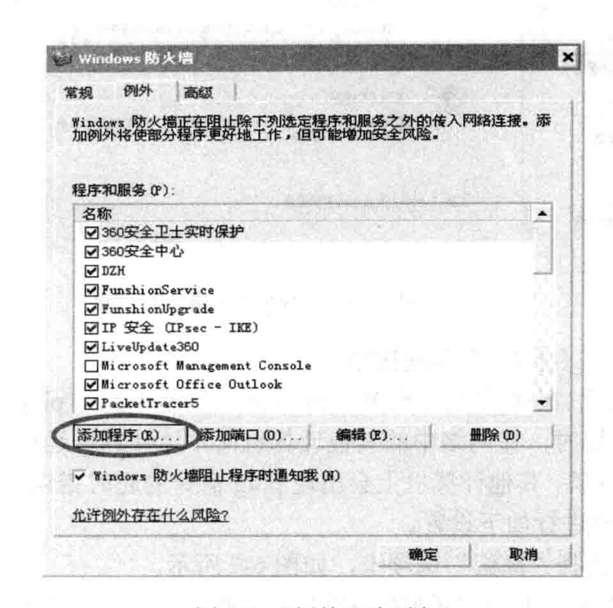


图 6-9 “例外”选项卡

图 6-10 “添加程序”对话框

④ 启用安全记录。

当 Windows 防火墙处于启动状态时，在默认情况下并不启用安全记录。但是，无论安全记录是否被启用，防火墙都能正常工作，而只有启用了 Windows 防火墙的连接才能使用日志记录功能。

步骤 1：在“Windows 防火墙”对话框中选择“高级”选项卡。

步骤 2：单击“安全日志记录”选项组中的“设置”按钮，打开“日志设置”对话框，选中“记录被丢弃的数据包”和“记录成功的连接”复选框，如图 6-11 和图 6-12 所示，再单击“确定”按钮。

⑤ 查看安全日志。

防火墙安全日志文件名为 pfirewall.log，默认情况下存放在 Windows 文件夹中，但必须选中“记录被丢弃的数据包”和“记录成功的连接”复选框后，才能使 pfirewall.log 文件出现在 Windows 文件夹中。

步骤 1：在“Windows 防火墙”对话框中选择“高级”选项卡。

步骤 2：单击“安全日志记录”选项组中的“设置”按钮，打开“日志设置”对话框。



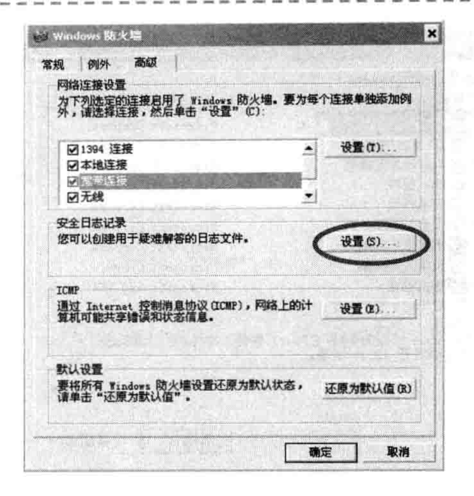




图 6-11　Windows 防火墙“高级”选项卡



图 6-12　“日志设置”对话框

步骤 3：单击“另存为”按钮，在打开的“另存为”对话框中找到并右击 pfirewall.log 文件，在弹出的快捷菜单中选择“打开”命令，即可查看安全日志，如图 6-13 所示。

（2）简易防火墙的配置。

下面将介绍在 Windows XP Professional 上配置简易防火墙的方法。

① 添加 IP 安全策略管理单元。

步骤 1：选择“开始”→“运行”命令，打开“运行”对话框，在“打开”文本框中输入“mmc”，单击“确定”按钮，打开“控制台 1”窗口，如图 6-14 所示，其中包含了“控制台根节点”窗口。

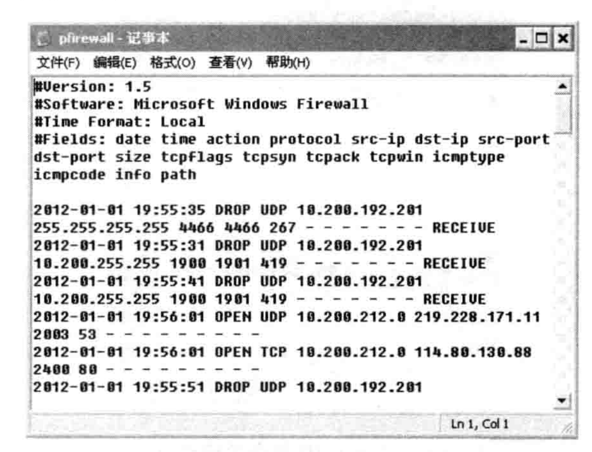


图 6-13　pfirewall.log 文件内容

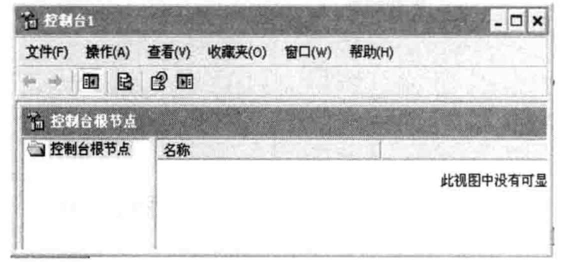


图 6-14　“控制台 1”窗口

步骤 2：在“控制台 1”窗口的“文件”菜单中选择“添加/删除管理单元”命令，打开“添加/删除管理单元”对话框，如图 6-15 所示，选择“独立”选项卡。

步骤 3：在“将管理单元添加到”下拉列表框中选择“控制台根节点”选项，然后单击“添加”按钮，打开“添加独立管理单元”对话框，如图 6-16 所示。

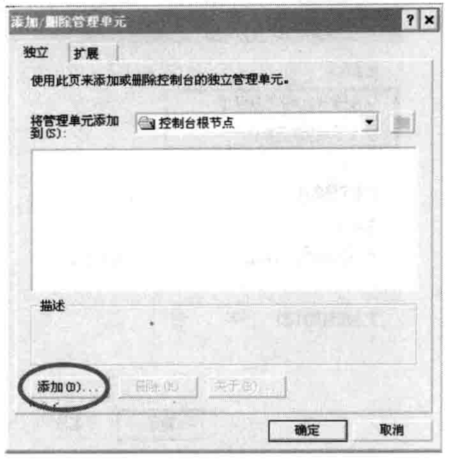





图 6-15 “添加/删除管理单元”对话框　　　图 6-16 “添加独立管理单元”对话框

步骤 4：在“可用的独立管理单元”列表框中选择“IP 安全策略管理”选项，然后单击“添加”按钮，打开“选择计算机或域”对话框，如图 6-17 所示。选中“本地计算机”单选按钮，再单击“完成”按钮，返回“添加独立管理单元”对话框。

步骤 5：单击“关闭”按钮，返回“添加/删除管理单元”对话框。

步骤 6：单击“确定”按钮，返回“控制台 1”窗口，完成“IP 安全策略，在本地计算机”的设置，如图 6-18 所示。

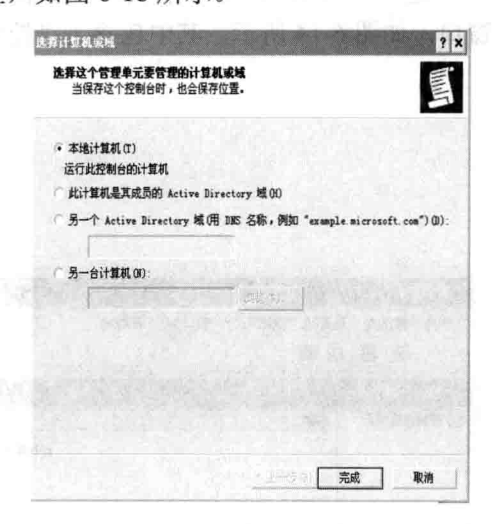


图 6-17 “选择计算机或域”对话框

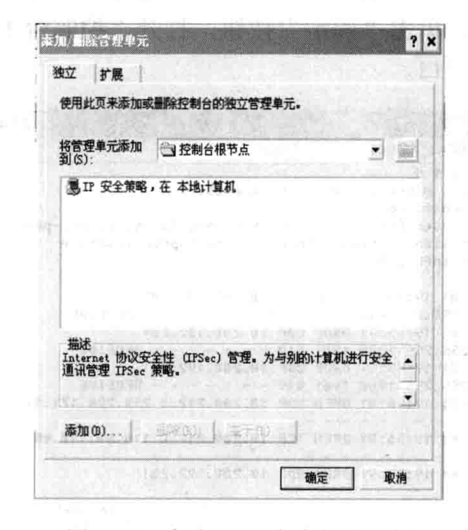


图 6-18 完成了 IP 安全策略添加

② 添加 IP 筛选器表。

在本机中添加一个能对指定 IP 地址（如 192.168.10.1）进行筛选的 IP 筛选器表。

步骤 1：在“控制台 1”窗口的“控制台根节点”窗口中右击“IP 安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”命令，打开“管理 IP 筛选器表和筛选器操作”对话框，如图 6-19 和图 6-20 所示，单击“添加”按钮。



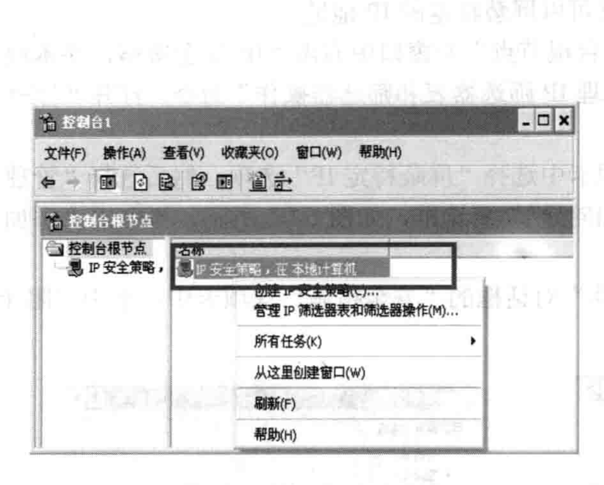


图 6-19　控制台根节点

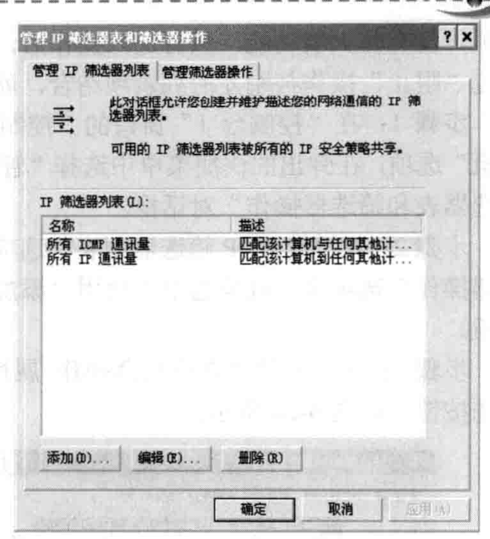


图 6-20　“管理 IP 筛选器表和筛选器操作”对话框

步骤 2：在打开的“IP 筛选器列表”对话框中，输入此 IP 筛选器名称和描述。例如，“名称”为“STIEI 屏蔽特定 IP”，“描述”为“STIEI 想屏蔽 192.168.10.1”，并取消选中“使用‘添加向导’”复选框，如图 6-21 所示，然后单击“添加”按钮。

步骤 3：在打开的“筛选器 属性”对话框中选择“寻址”选项卡，在“源地址”和“目标地址”下拉列表框中分别选择“我的 IP 地址”和“一个特定的 IP 地址”选项。在“IP 地址”文本框中输入要屏蔽的 IP 地址，如 192.168.10.1，如图 6-22 所示。

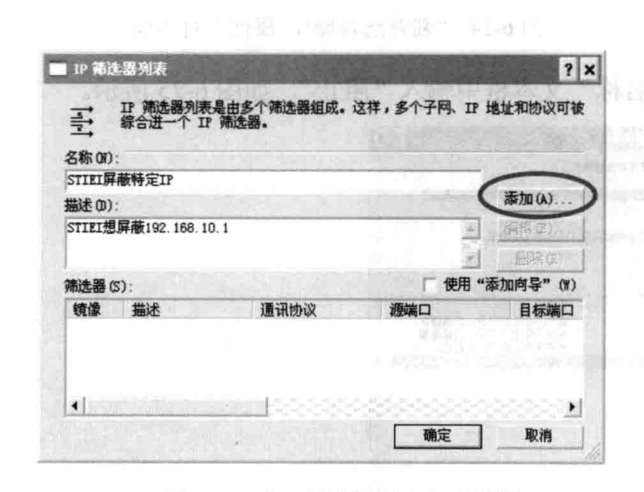


图 6-21　“IP 筛选器列表”对话框

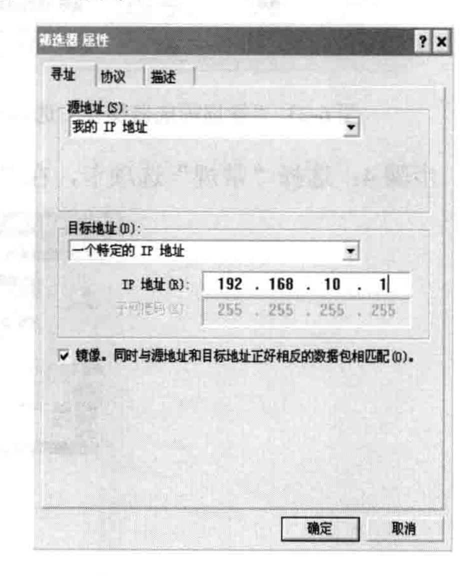


图 6-22　协议及端口设定

③ 添加 IP 筛选器操作。

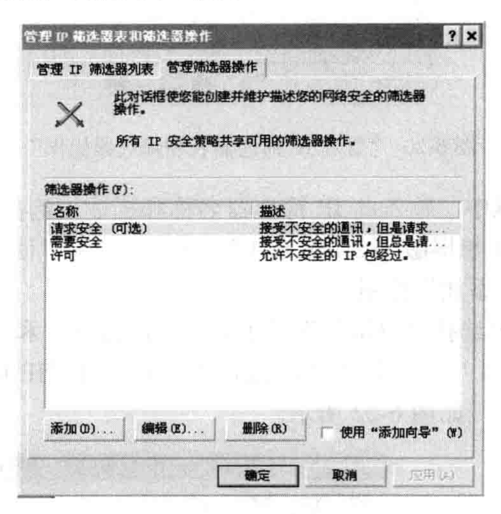
上述操作将一个虚拟的 C 类网址 192.168.10.1 添加到了待屏蔽 IP 列表中，但它只是一个列

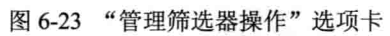
表项，没有防火墙功能，只有加入操作后，才能够发挥作用。下面将建立一个“阻止”操作，通过“阻止”操作与刚才的列表项结合，就可以屏蔽特定的 IP 地址。

步骤 1：在“控制台 1”窗口的“控制台根节点”左窗口中右击“IP 安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”命令，打开“管理 IP 筛选器表和筛选器操作”对话框。

步骤 2：在“管理 IP 筛选器列表”选项卡中选择“屏蔽特定 IP”选项，然后选择“管理筛选器操作”选项卡，取消选中“使用‘添加向导’”复选框，如图 6-23 所示，再单击“添加”按钮。

步骤 3：在打开的“新筛选器操作 属性”对话框的“安全措施”选项卡中，选中“阻止”单选按钮，如图 6-24 所示。




图 6-23 “管理筛选器操作”选项卡

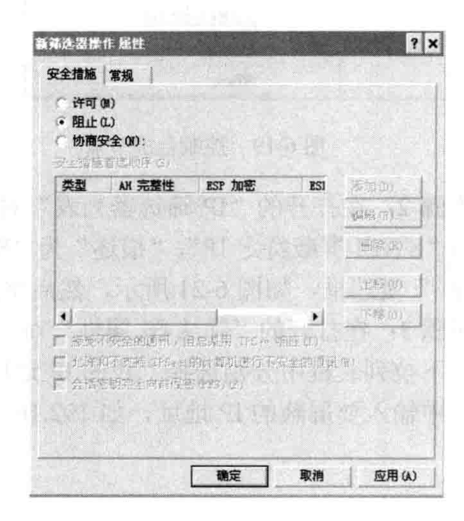


图 6-24 “新筛选器操作 属性”对话框

步骤 4：选择“常规”选项卡，在“名称”文本框中输入“阻止”，如图 6-25 所示。

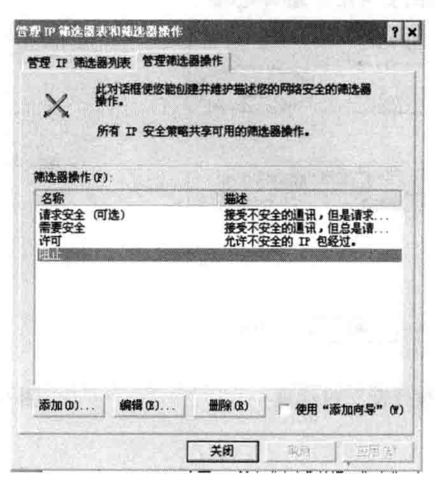


图 6-25 “阻止”添加到列表中



步骤 5：单击“确定”按钮，此时“阻止”操作就添加到“筛选器操作”列表中了。

步骤 6：单击“关闭”按钮，完成本次操作。

④ 创建 IP 安全策略。

筛选器表和筛选器操作已建立完毕，将它们结合起来发挥防火墙的作用。

步骤 1：返回“控制台 1”窗口，在“控制台根节点”窗口中右击“IP 安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“创建 IP 安全策略”命令，打开“IP 安全策略向导”对话框，如图 6-26 所示。

步骤 2：单击“下一步”按钮，出现“IP 安全策略名称”界面，如图 6-27 所示，在“名称”文本框中输入“STIEI 的 IP 安全策略”，还可以在“描述”文本框中输入对安全策略设置的描述。

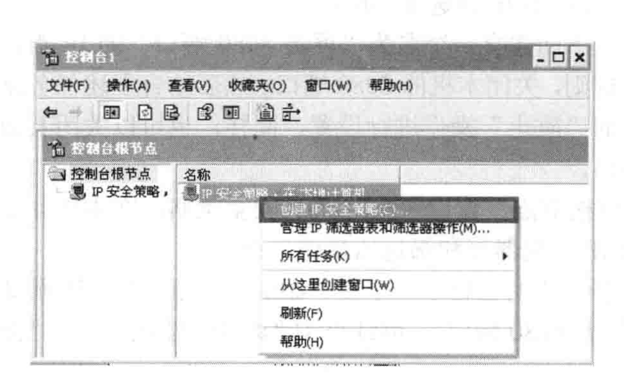


图 6-26　创建 IP 安全策略

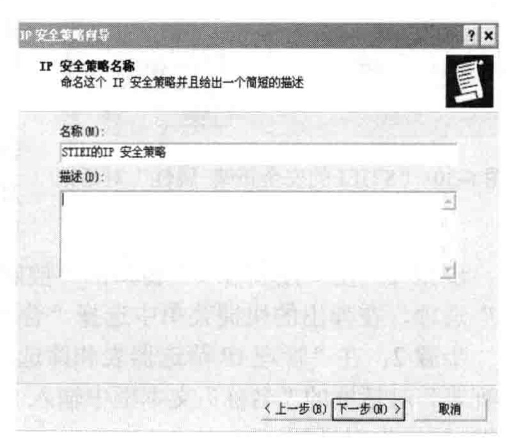


图 6-27　“IP 安全策略名称”界面

步骤 3：单击“下一步”按钮，出现“安全通讯请求”界面，如图 6-28 所示，取消选中“激活默认响应规则”复选框。

步骤 4：单击“下一步”按钮，出现“正在完成 IP 完全策略向导”界面，如图 6-29 所示。选中“编辑属性”复选框，再单击“完成”按钮。

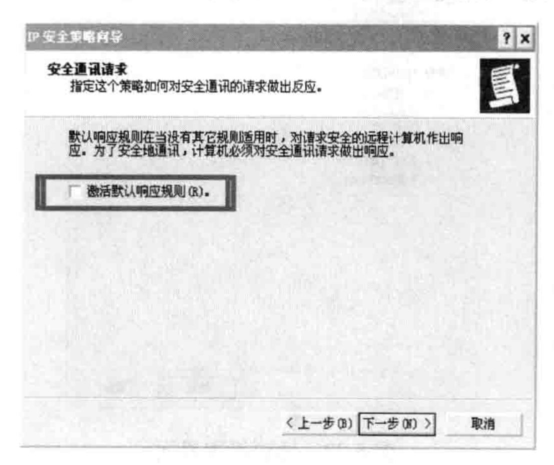


图 6-28　“安全通讯请求”界面

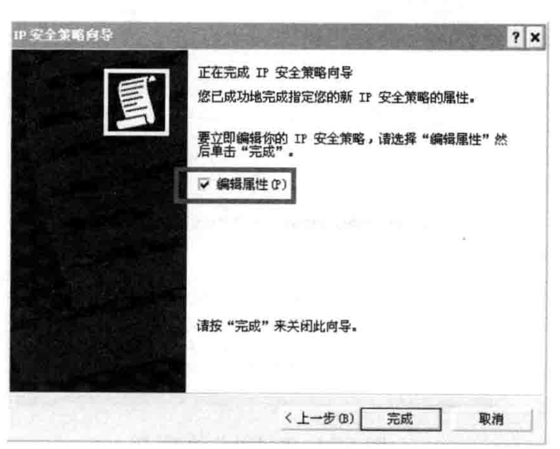


图 6-29　完成安全策略向导

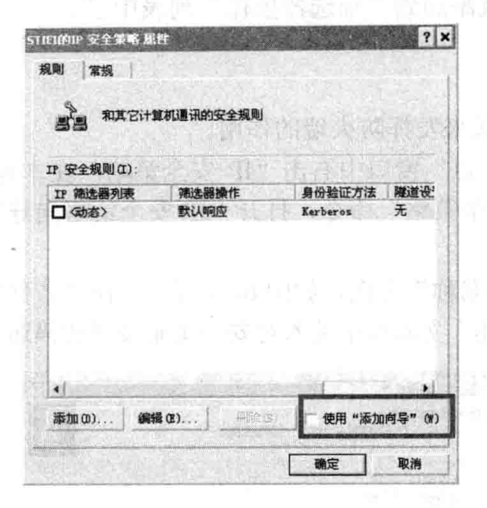


图 6-30 “STIEI 的安全策略 属性”对话框

步骤 5：在打开的“STIEI 的安全策略 属性”对话框中选择“规则”选项卡，取消选中“使用‘添加向导’”复选框，再单击“添加”按钮，如图 6-30 所示，打开“新规则 属性”对话框。

步骤 6：在“IP 筛选器列表”选项卡中选中新建立的 IP 筛选器（即“屏蔽特定 IP”）单选按钮，再在“筛选器操作”选项卡中选中“阻止”单选按钮，然后单击“确定”按钮，返回“STIEI 的安全策略 属性”对话框，可以看到新规则已经建立。单击“关闭”按钮，至此，屏蔽特定 IP 的操作就完成了。

⑤ 用 IP 筛选器屏蔽特定端口。

下面建立一个名为“屏蔽 8080 端口”的 IP 筛选器规则，关闭本机的 8080 端口，然后结合上述任务添加的“阻止”操作进行设置。同样，也可以关闭其他端口。

步骤 1：在“控制台 1”窗口的“控制台根节点”窗口中右击“IP 安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“管理 IP 筛选器表和筛选器操作”命令。

步骤 2：在“管理 IP 筛选器表和筛选器操作”对话框中，单击“添加”按钮，在“IP 筛选器列表”对话框的“名称”文本框中输入“屏蔽 8080 端口”，继续单击“添加”按钮，打开“筛选器 属性”对话框。

步骤 3：选择“寻址”选项卡，在“源地址”下拉列表框中选择“任何 IP 地址”选项；在“目标地址”下拉列表框中选择“我的 IP 地址”选项；取消选中“镜像”复选框，如图 6-31 所示。同时，也可对选定的通信协议屏蔽，如图 6-32 所示。

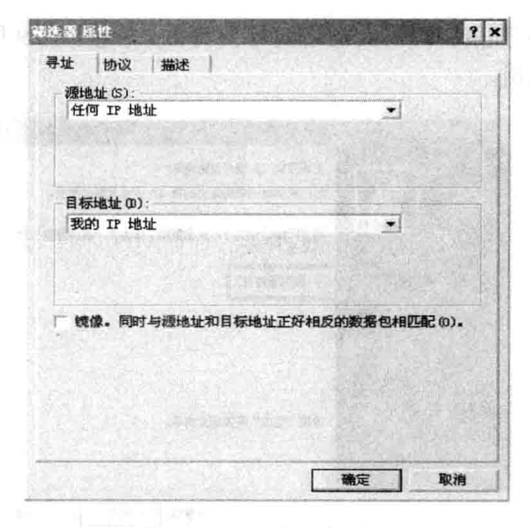


图 6-31 “寻址”选项卡

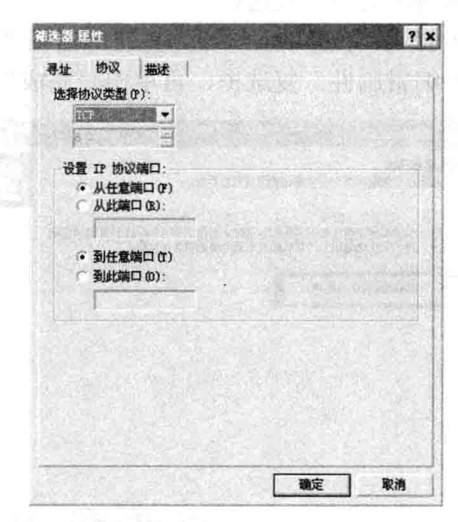


图 6-32 协议设置界面



步骤 4：单击“确定”按钮，返回“IP 筛选器列表”对话框，再单击“确定”按钮，返回“管理 IP 筛选器表和筛选器操作”对话框，可以看到“屏蔽 8080 端口”筛选器已建立完成（见图 6-33）。单击“关闭”按钮。

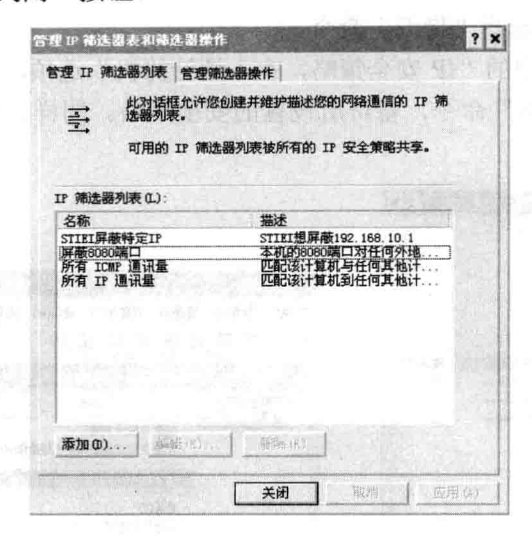


图 6-33 屏蔽端口操作已完成

⑥ 应用 IP 安全策略规则。

步骤 1：在“控制台 1”窗口的“控制台根节点”窗口中右击新建立的“STIEI 的 IP 安全策略”选项，在弹出的快捷菜单中选择“属性”命令，打开“STIEI 的 IP 安全策略 属性”对话框，单击“添加”按钮，打开“新规则 属性”对话框，如图 6-34 和图 6-35 所示。

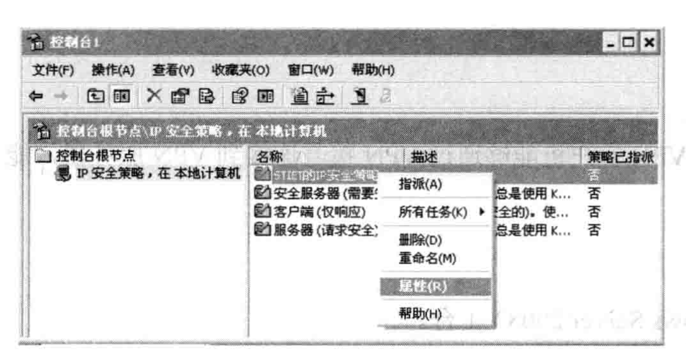


图 6-34 选择“STIEI 的 IP 安全策略”的“属性”命令

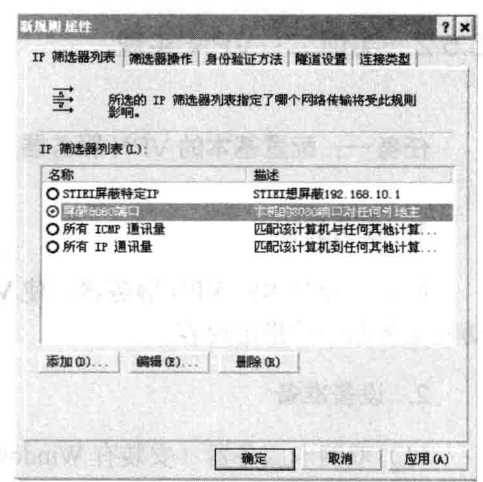


图 6-35 “新规则 属性”对话框

步骤 2：在“IP 筛选器列表”选项卡中，选中新建立的 IP 筛选器（即“屏蔽 8080 端口”）单选按钮，再在“筛选器操作”选项卡中选中“阻止”单选按钮，然后单击“确定”按钮，返回“STIEI 的 IP 安全策略 属性”对话框，可以看到新规则已经建立。至此，共有两条安全规

则（“STIEI 屏蔽特定 IP”和“屏蔽 8080 端口”）已经建立，如图 6-36 所示。单击“关闭”按钮，返回“控制台 1”窗口。

步骤 3：在“控制台 1”窗口的“控制台根节点”窗口中单击“STIEI 的 IP 安全策略”选项，在弹出的快捷菜单中选择“指派”命令。

步骤 4：右击左窗口中的“IP 安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“所有任务”→“导出策略”命令，备份所设置的安全策略。同样，也可以使用“导入策略”命令恢复，如图 6-37 所示。

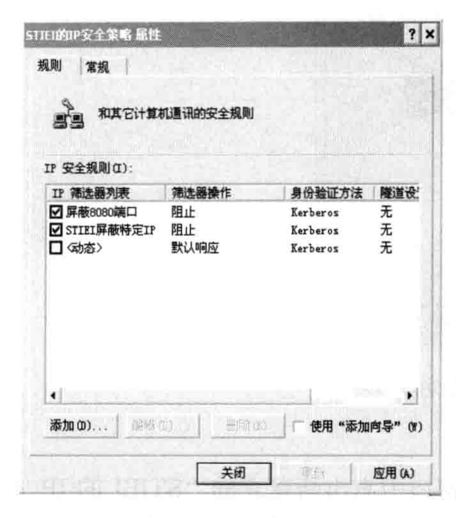


图 6-36　两个安全规则已建立

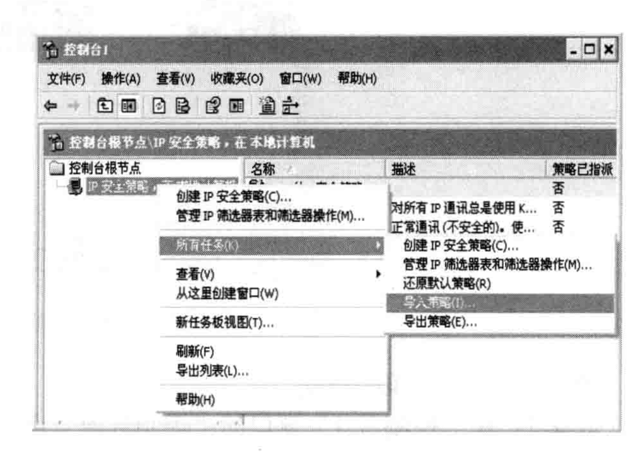


图 6-37　安全策略导入与导出

6.5.2　实训二：VPN 实现

任务一：配置基本的 VPN 服务器

1. 任务目标

配置一台基本的 VPN 服务器，使 VPN 客户机能够通过 VPN 拨号连接到 VPN 服务器，能访问服务器中的指定内容。

2. 设备准备

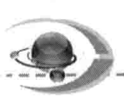
（1）双网卡服务器（安装有 Windows Server 2008）1 台。

（2）客户机和交换机各 1 台。

（3）直通线两根。

3. 网络拓扑结构

为完成本次实训任务，搭建图 6-38 所示的网络拓扑结构。



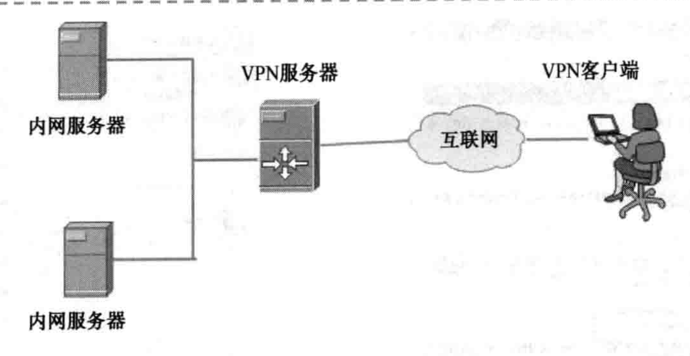


图 6-38　网络拓扑结构图

4. 任务实施

（1）硬件连接。

用两根直通线分别把服务器（连接外网的网卡）和客户机连接到交换机上。

（2）TCP/IP 协议配置。

步骤 1：配置 VPN 服务器的两块网卡的 IP 地址参数如表 6-4 所示。

表 6-4　网卡 IP 地址参数

网卡名称	IP 地址	子网掩码
外网	200.10.10.10	255.255.255.0
内网	192.168.10.2	255.255.255.0
客户端	200.10.10.20	255.255.255.0

步骤 2：在服务器和客户机之间用 ping 命令测试网络的连通性。

（3）关闭防火墙和 ICS 服务。

要在服务器上启用 Windows Server 2008 的 VPN 服务，必须先关闭系统自带的一些服务。

步骤 1：关闭默认防火墙。

选择“开始”→“设置”→“控制面板”命令，打开“控制面板”窗口，然后双击其中“Windows 防火墙”图标，打开“Windows 防火墙”对话框，如图 6-39 所示。

步骤 2：禁用 ICS 服务。

选择“开始”→“管理工具”→“属性（本地）”→“Windows Firewall/Internet Connection Sharing”命令，“启用类型”选为“禁用”。

（4）安装“路由与远程访问”管理工具。

步骤 1：在“开始”菜单中选择“服务器管理器”选项（见图 6-40），在打开的“服务器管理器”界面中选择“角色”→“添加角色”选项，如图 6-41 所示。

步骤 2：在“添加角色向导”对话框中选择“服务器角色”，勾选“网络策略与访问服务”复选框（见图 6-42），在“角色服务”属性中选择“路由和远程访问服务”复选框（见图 6-43），最后，确认安装。如图 6-44 所示。

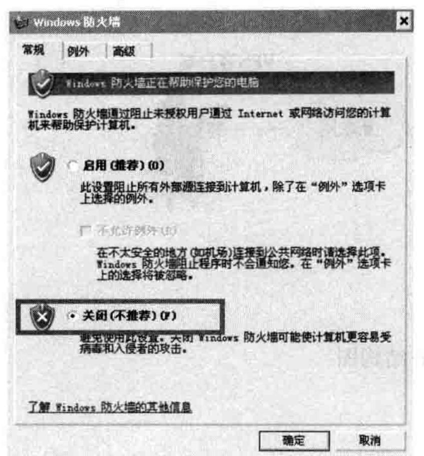


图 6-39　关闭防火墙

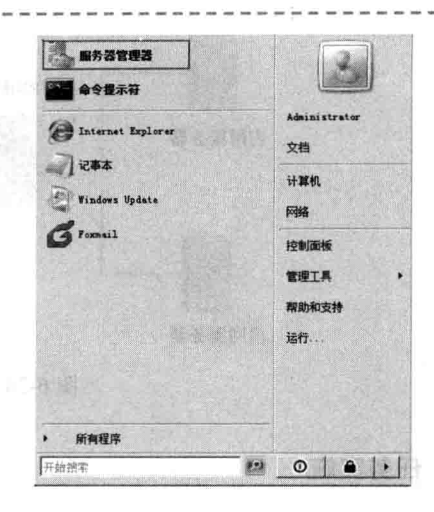


图 6-40　启动“服务器管理器”程序



图 6-41　“服务器管理器”界面

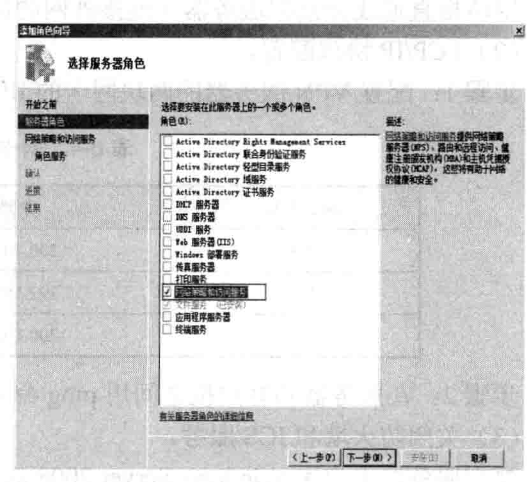


图 6-42　添加服务器角色向导

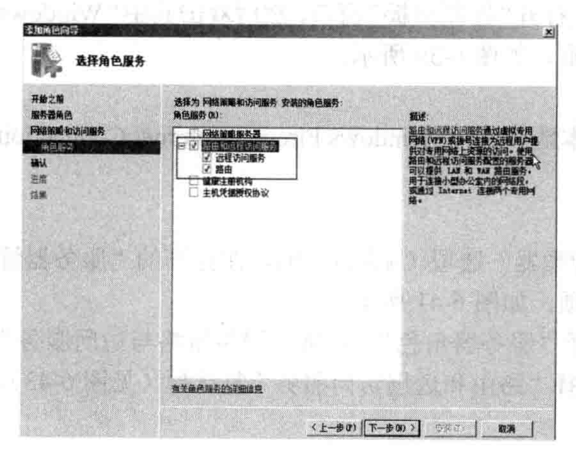


图 6-43　选择“路由和远程访问服务”

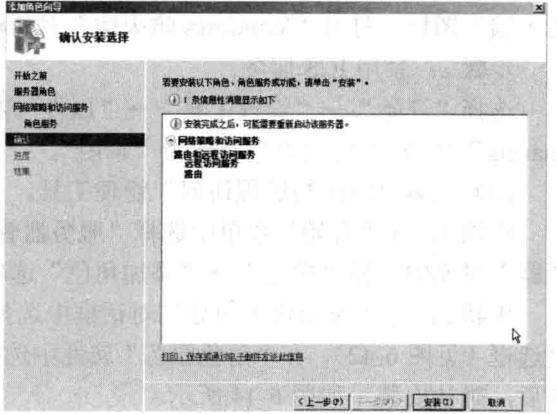


图 6-44　确认安装选择

步骤 3：安装完成后，选择“控制面板”→“管理工具”→“路由和远程访问”命令，打开“路由和远程访问”控制台，右击“SERVER”，在弹出的快捷菜单中选择“配置并启用路由和远程访问”命令，如图 6-45 所示。

步骤 4：在打开的“路由和远程访问服务器安装向导”对话框中，单击“下一步”按钮，出现“配置”界面，选中“远程访问（拨号或 VPN）”单选按钮，如图 6-46 所示。

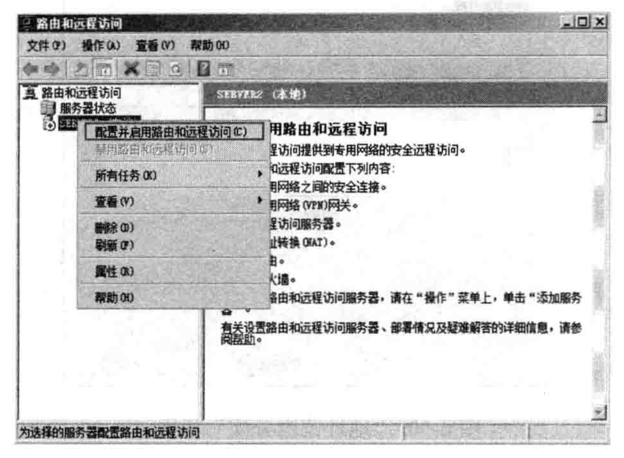


图 6-45　启用路由和远程访问

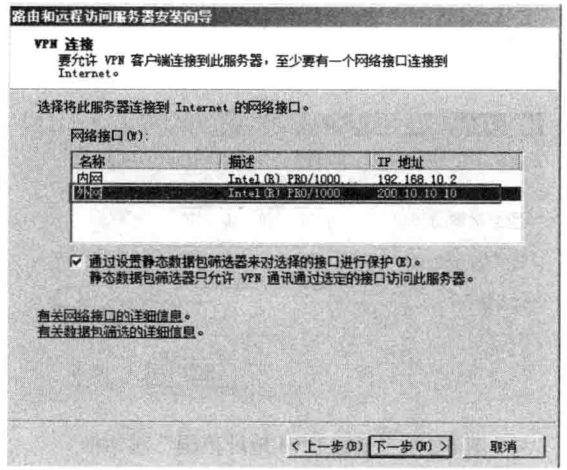


图 6-46　“配置”界面

步骤 5：单击“下一步”按钮，出现“远程访问”界面，选中 VPN 复选框，如图 6-47 所示。

步骤 6：单击“下一步”按钮，出现如图 6-48 所示的“VPN 连接”界面，选择 VPN 接入端口（即连接外网的网卡），注意启用 VPN 的接口应该是连接互联网的接口，如果选择图中的复选框，则此网络接口只允许通过以 VPN 方式传输过来的数据包，其他方式传输过来的数据包将全部被删除。

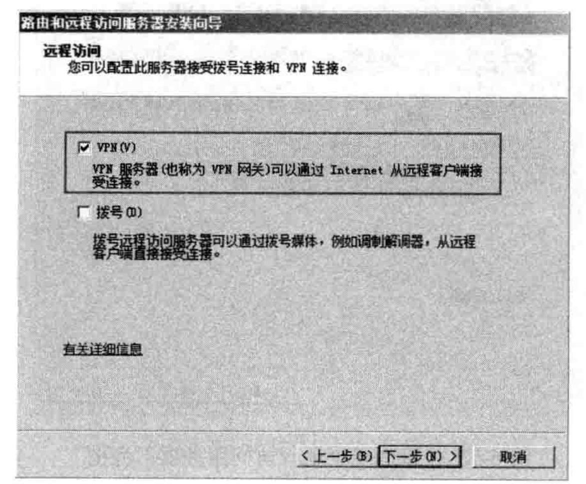


图 6-47　“远程访问”界面

图 6-48　“VPN 连接”界面

步骤 7：单击“下一步”按钮，出现“IP 地址分配”界面，显示如何为接入的客户端分配地址，接入的客户端将被分配一个可以在内网中直接使用的地址，这里选择第二项，由管理员进行配置地址范围（见图 6-49）。

步骤 8：单击“下一步”按钮，出现“地址范围分配”界面，如图 6-50 所示。

图 6-49 “IP 地址分配”界面

图 6-50 “地址范围分配”界面

步骤 9：单击“新建”按钮，在打开的“新建 IPv4 地址范围”对话框中，输入“起始 IP 地址”为 192.168.10.100，“结束 IP 地址”为 192.168.10.110，共 11 个地址，如图 6-51 所示。

步骤 10：单击“确定”按钮，返回“地址范围分配”界面。再单击“下一步”按钮，出现“管理多个远程访问服务器”界面，选中“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮，如图 6-52 所示。

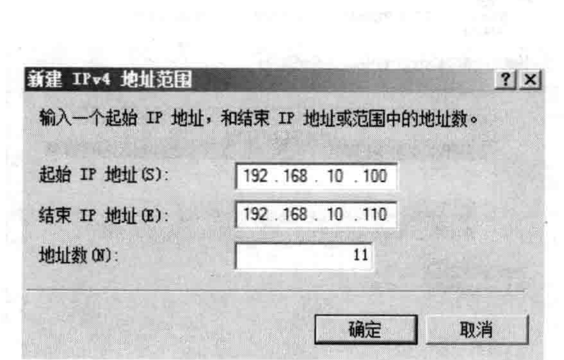


图 6-51 “新建 IPv4 地址范围”对话框

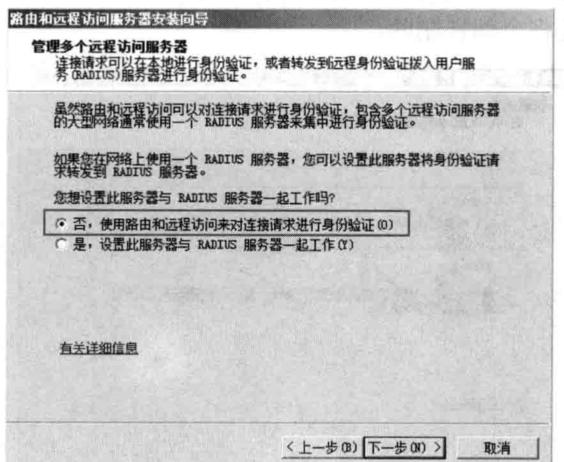


图 6-52 “管理多个远程访问服务器”界面

步骤 11：单击“下一步”按钮，再单击“完成”按钮。然后开启 DHCP 中继（见图 6-53），单击“确定”按钮，至此，路由和远程访问建立完成，如图 6-54 所示。



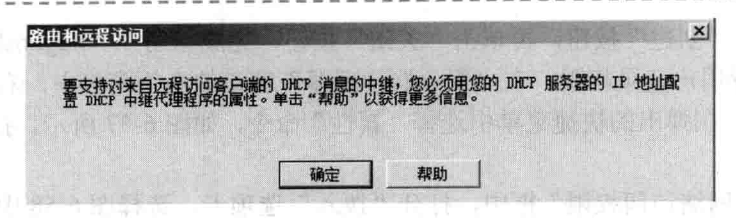


图 6-53　启用 DHCP

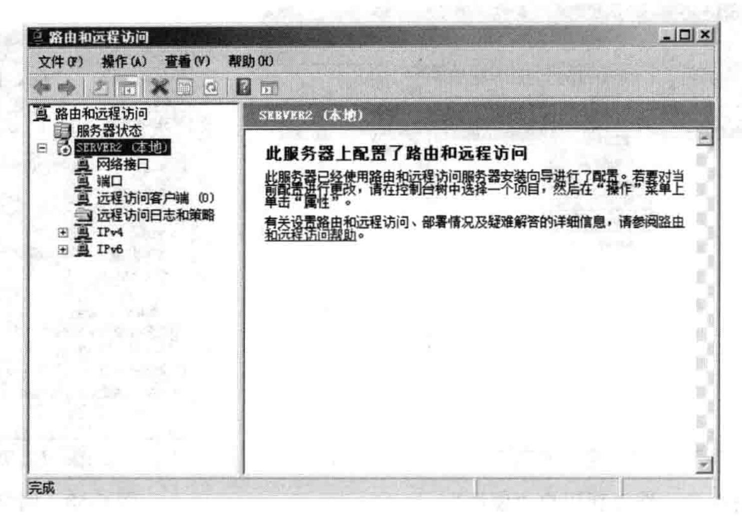


图 6-54　完成设置后的界面

（5）在 VPN 服务器上配置 VPN 登录用户。

步骤 1：右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，打开“服务器管理器”窗口，依次展开“系统工具”→“本地用户和组”→“用户”选项，在右侧窗格的空白处右击，在弹出的快捷菜单中选择“新用户”命令，如图 6-55 所示。

步骤 2：在打开的“新用户”对话框中，添加本地用户账户：用户名“huguosheng”和密码“123456”，并选中下方的“用户不能更改密码”和“密码永不过期”复选框，如图 6-56 所示。

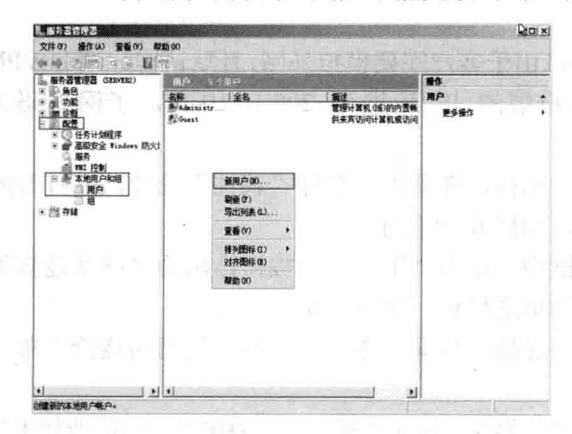


图 6-55　“服务器管理器”窗口

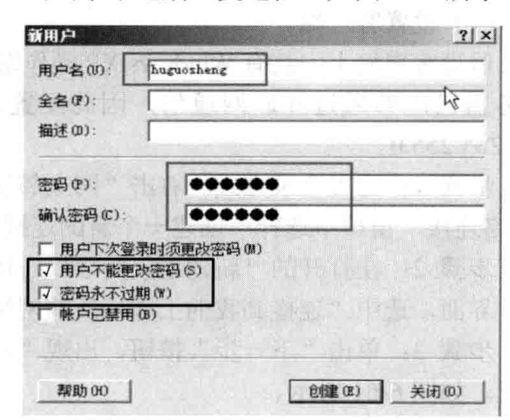


图 6-56　“新用户”对话框

步骤 3：单击“创建”按钮，再单击“关闭”按钮，完成新用户“huguosheng”的创建。

步骤 4：配置用户登录权限。在“服务器管理器”窗口的右侧窗格中，右击刚创建的新用户“huguosheng”，在弹出的快捷菜单中选择“属性”命令，如图 6-57 所示，打开“huguosheng 属性”对话框。

步骤 5：在“网络访问权限”框中，打开“拨入”选项卡，选择图 6-58 中“允许访问”单选按钮后，单击“确定”按钮。



图 6-57 选择新用户“属性”

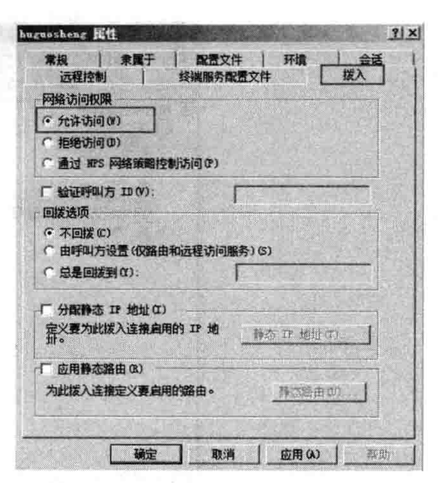


图 6-58 网络访问权限

任务二：配置 VPN 客户端

1. 任务目标

能正确配置客户端，并在客户端拨号接入 VPN 服务器。

2. 任务实施

（1）设置客户端。

假设客户机上安装有 Windows XP 操作系统。由于客户端要模拟外网，且默认客户端和 VPN 服务器已能够通过互联网通信，因此配置客户端的 IP 地址为 200.10.10.20，子网掩码为 255.255.255.0。

步骤 1：配置登录方式。右击“网上邻居”图标，在菜单中选择“属性”选项，在打开的“网络连接”窗口中选择“创建一个新的连接”，如图 6-59 所示。

步骤 2：在打开的“新建连接向导”对话框中，单击“下一步”按钮，出现“网络连接类型”界面，选中“连接到我的工作场所的网络”单选按钮，如图 6-60 所示。

步骤 3：单击“下一步”按钮，出现“网络连接”界面，选中“虚拟专用网络连接”单选按钮，如图 6-61 所示。

步骤 4：单击“下一步”按钮，出现“连接名”界面，输入连接名：上海电子信息职业技术学院，如图 6-62 所示。因为默认客户端已经连接到互联网，所以在图 6-63 中选择“不拨初始连接”。



步骤5：单击“下一步”按钮，出现“VPN 服务器选择”界面（见图6-64），输入VPN服务器的IP地址，如200.10.10.10。

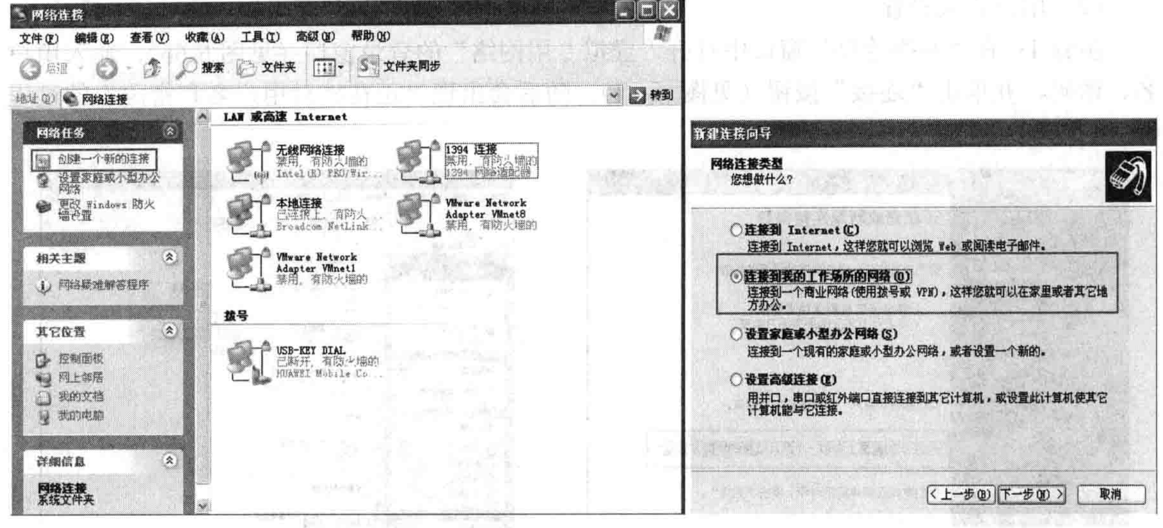


图6-59　“网络连接”窗口　　图6-60　“网络连接类型”界面

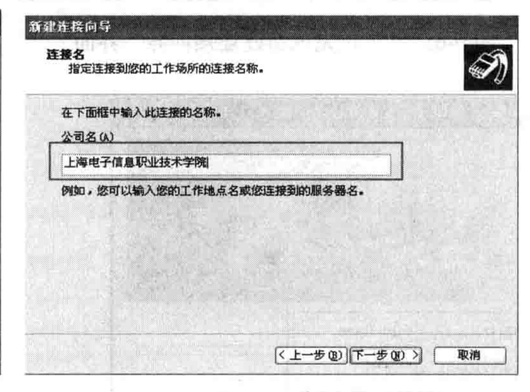


图6-61　“网络连接”界面　　图6-62　“连接名”界面

图6-63　“公用网络”拨号选择　　图6-64　“VPN 服务器选择”界面

步骤 6：单击“下一步”按钮，出现“正在完成新建连接向导”界面，选中“在我的桌面上添加一个到此连接的快捷方式”复选框，如图 6-65 所示。单击“完成”按钮。

（2）用户登录设置。

步骤 1：在“网络连接”窗口中打开“虚拟专用网络”的登录窗口（见图 6-66），输入用户名、密码，并单击“连接”按钮（见图 6-67），随后会出现“正在核对用户名和密码”的过程（见图 6-68）。

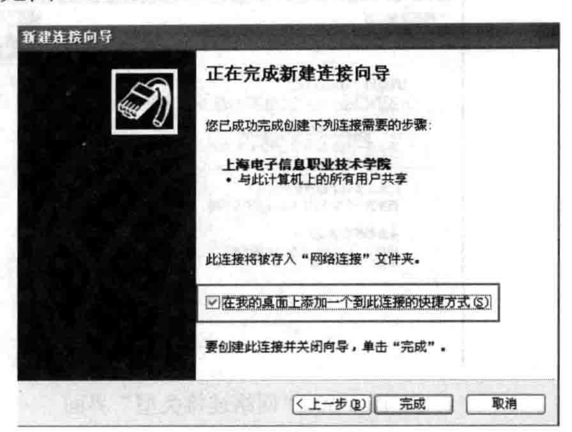


图 6-65 “正在完成新建连接向导”界面

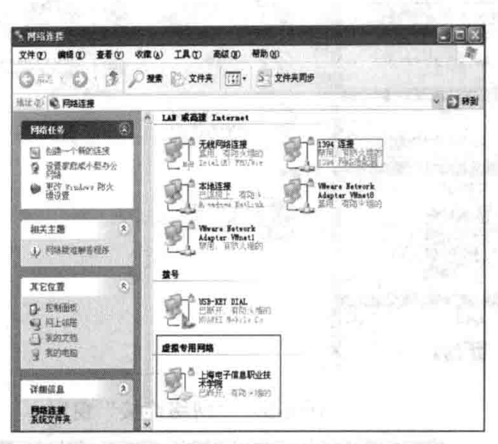


图 6-66 “网络连接”界面中“虚拟专用网络”



图 6-67 输入用户名、密码界面

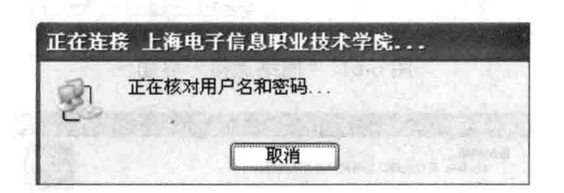
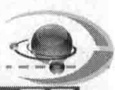


图 6-68 身份验证界面

步骤 2：身份验证后，“网络连接”窗口中可以看到“虚拟专用网络”已经连接成功（见图 6-69）。

步骤 3：右击图 6-69 中的“虚拟专用网络”图标，打开状态对话框，选择“详细信息”选项卡，如图 6-70 所示。从图中可以看出，此时客户端获得了一个新的 IP 地址 192.168.10.101。之后就可以通过 VPN 服务器的 IP 地址访问 VPN 服务器了，就像访问本地局域网一样。





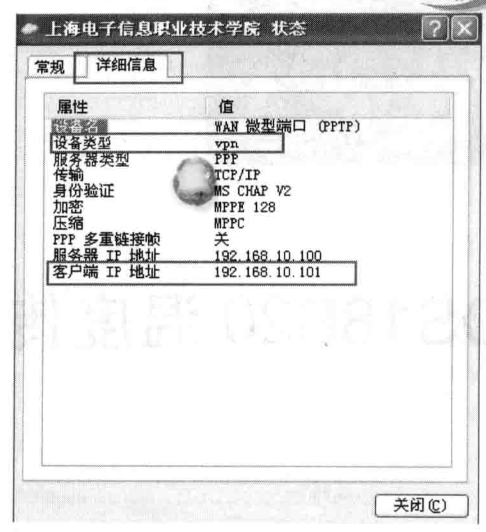


图 6-69　虚拟专用网络安装成功

图 6-70　状态对话框

（3）登录测试。

在客户端上选择“开始”→“运行”命令，在打开的“运行”对话框中输入“\\IP 地址”的方式访问内网中的某一台计算机上的共享文件夹，这里用 192.168.10.1 这台计算机上的共享文件夹“web1”来测试，如图 6-71 和图 6-72 所示。

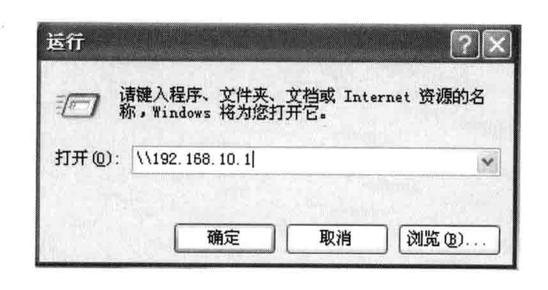


图 6-71　“运行”对话框

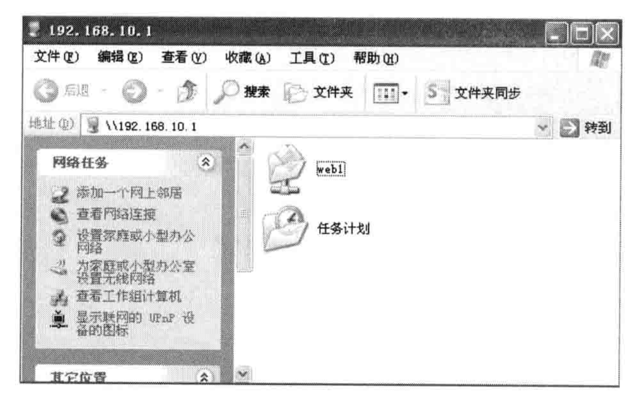


图 6-72　共享 192.168.10.1 主机的文件夹

6.6 练习题

1．通过网络查找物联网技术应用的利弊分析，并通过 PPT 汇报。

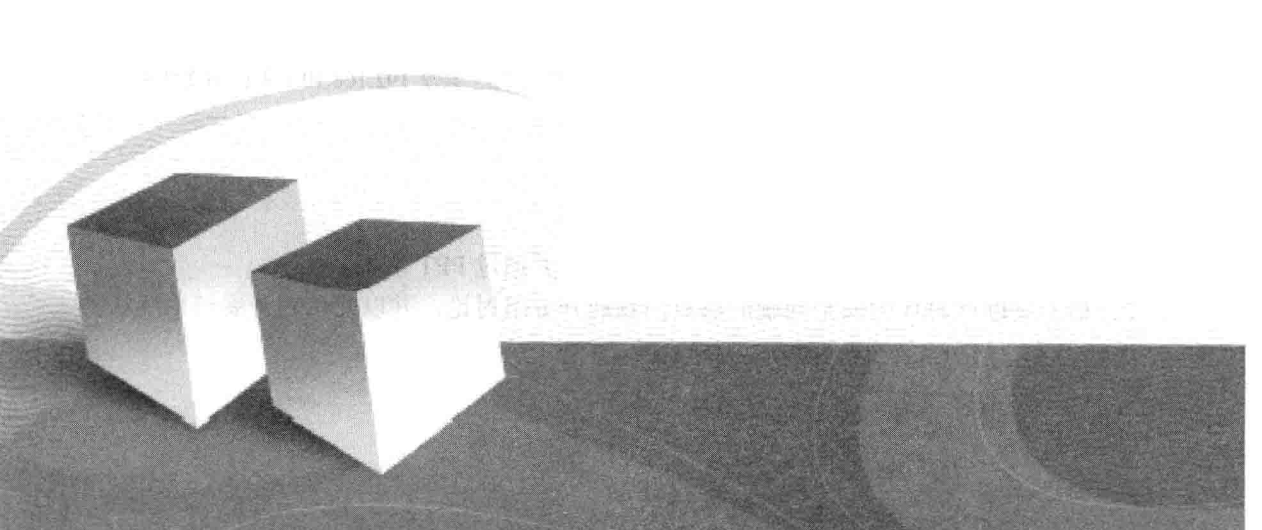
2．借助物联网时代的安全问题的热点问题展开分组讨论，并以此话题开展辩论赛活动。

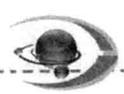
附录 A

DS18B20 温度传感器介绍

DS18B20 是美国 DALLAS 公司推出的数字温度传感器，将温度传感器、数字转换电路集成到了一起，外形如同一只三极管。

DS18B20 的测温范围为−55℃～125℃，12 位温度读数，分辨率为 1/16℃，温度转换间最多为 750ms。





一、DS18B20 的引脚功能

DS18B20 的引脚图如图 A-1 所示。

DQ：数据输入输出，可直接与单片机的 I/O 口相连。

VDD：+5V 电源电压。

GND：电源地。

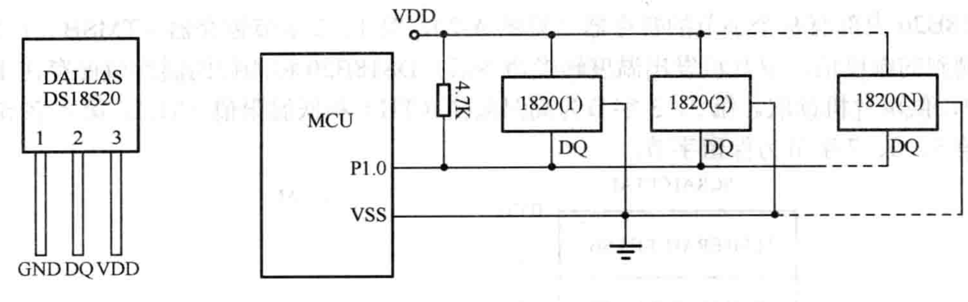
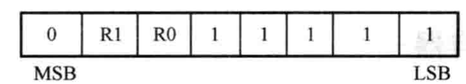


图 A-1　DS18B20 引脚

二、DS18B20 的序列号

每片 DS18B20 均有一个唯一产品序列号，固化在内部的 64 位激光 ROM 中，其格式为：



（1）开始 8 位是产品的类型编号（工厂代码）。

（2）接着是每个器件唯一的序号，共 48 位。

（3）最后 8 位是针对前面 56 位的 CRC 校验码。

这也是多个 DS18B20 可以采用一条数据线进行通信的原因，只要单片机用匹配命令即可访问总线上的指定 DS18B20。

三、DS18B20 的配置寄存器

0	R1	R0	1	1	1	1	1

MSB　　　　　　　　LSB

第五位是 1。TM 是测试模式位，用于设置 DS18B20 在工作模式还是在测试模式，在 DS18B20 出厂时该位被设置为 0，用户不要去改动。R1 和 R0 用来设置分辨率（见表 A-1）。

表 A-1　R1 和 R0 位设置值

R1	R0	Thermometer Resolution	Max Conversion Time
0	0	9 bit	93.75 ms　($t_{conv}/8$)
0	1	10 bit	187.5 ms　($t_{conv}/4$)

续表

R1	R0	Thermometer Resolution	Max Conversion Time
1	0	11 bit	375 ms　（$t_{conv}/2$）
1	1	12 bit	750 ms　（t_{conv}）

四、DS18B20 的温度暂存器

DS18B20 内部有 9 个字节的暂存器（见图 A-2），第 1、2 字节暂存器（TMSB、TLSB）存放当前测到的温度值，单片机发出温度转换命令后，DS18B20 将测得的温度值保存在 TMSB、TLSB 中，供单片机读取。第 2、3 字节为高温限值（TH）和低温限值（TL）。第 4 字节配置寄存器。第 5、6、7 字节为保留字节。

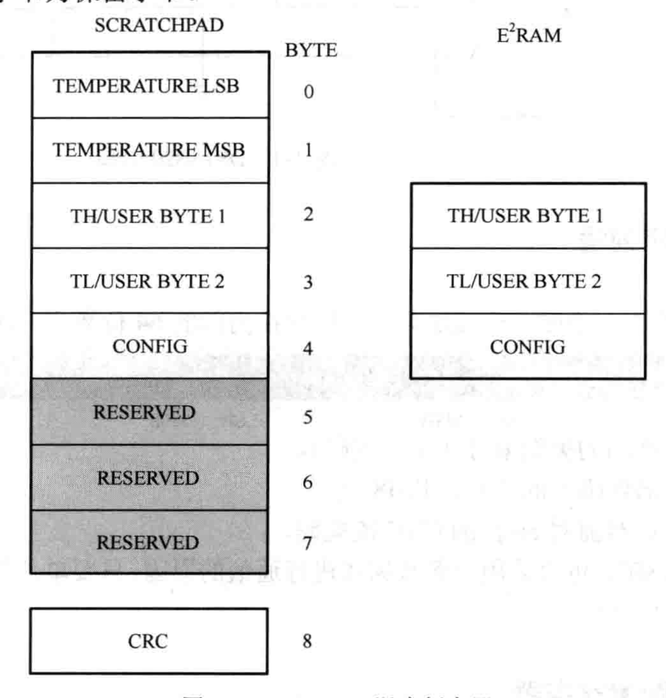


图 A-2　DS18B20 温度暂存器

五、DS18B20 的温度暂存器

DS18B20 出厂时被设置为 12。用 16 位符号扩展的二进制补码读数形式提供 0.0625℃/LSB 形式表达，其中 S 为符号位。

	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
LS Byte	2^3	2^2	2^1	2^0	2^{-1}	2^{-2}	2^{-3}	2^{-4}
	bit 15	bit 14	bit 13	bit 12	bit 11	bit 10	bit 9	bit 8
MS Byte	S	S	S	S	S	2^6	2^5	2^4



温度与数字量对应关系见表 A-2。

表 A-2　温度与数字量对应关系表

温度值（℃）	给出二进制码	十六进制表示
+125	0000　0111　1101　0000	07D0H
+25.0625	0000　0001　1001　0001	0191H
+0.5	0000　0000　0000　1000	0008H
0	0000　0000　0000　0000	0000H
−0.5	1111　1111　1111　1000	FFF8H
−25.0625	1111　1110　0110　1111	FE6FH
−55	1111　1100　1001　0000	FC90H

六、DS18B20 温度传感器数据采集指令格式

发送读取 DS18B20 温度传感器数据请求：

02	07	CB	01	00	D3	30	00	00	09

串口接收对象：0xCB　//表示协调器。

网络地址：0x0001　//表示读取网络地址为 0001 节点的数据，若需要采集其他节点的板载温度，则需要将网络地址更改为其他节点的网络地址。

数据对象：0xD3　//表示读取终端节点信息。

命令标识：0x0030　//表示读取终端节点的板载温度。

数据负荷长度为 0。

返回温度数据：

02	09	CB	01	00	D3	30	00	02	A2	00	0C

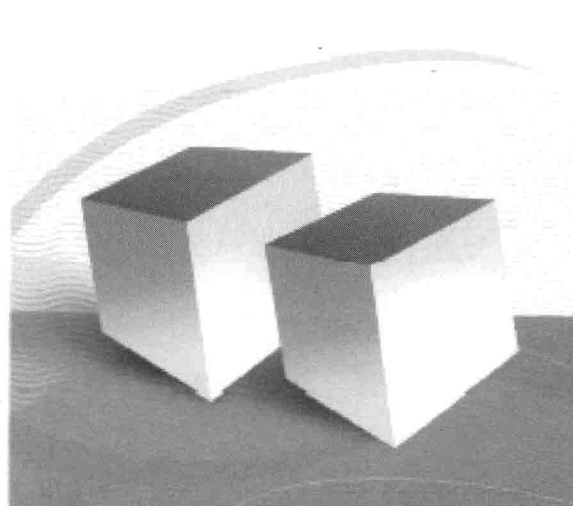
数据负荷长度：0x02，表示返回的数据负荷长度为 2 个字节。

数据负荷：0x00A2，表示+10.125℃。

温度数据格式参考 DS18B20 格式。

附录 B

CH-GWB301 蓝牙/WiFi/GPRS 节点参考指令





一、蓝牙配置命令

本组命令只能通过RS232接口且蓝牙串口未连接情况下操作，且所有命令配置后永久保存，直至重新配置为止，配置完成后通过 AT+RESET 指令重启模块后生效。若蓝牙串口已经连接，也可以用 AT+RESET 重启模块，重启后蓝牙处于未连接状态下，再进行相关操作。

1．AT+PIN：蓝牙配对密码设置。AT+PIN 后紧接 4 位配对密码，限数字，字符无效。

例：AT+PIN1234

返回 <CR><LF>AT+PIN1234[空格]OK<CR><LF> 配置正确

<CR><LF>AT+PIN1234[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

2．AT+NAME：设备名称设置。AT+NAME 后面紧接 20 位以内的数字或字符。

例：AT+NAMEBuletooh1

返回 <CR><LF>AT+NAMEBuletooh1[空格]OK<CR><LF> 配置正确

<CR><LF>AT+NAMEBuletooh1[空格]ERROR<CR><LF>配置错误

<CR><LF>ERROR<CR><LF>命令错误

3．AT+VERSION：蓝牙版本号查询。

例：AT+VERSION

返回：<CR><LF>AT+VERSION[空格]linvor1.5<CR><LF>返回正确 linvor1.5 为版本号

<CR><LF>AT+VERSION[空格]ERROR<CR><LF> 返回错误

<CR><LF>ERROR<CR><LF>命令错误

二、WiFi 配置命令

本组命令只能通过 RS232 接口操作，且所有命令配置后永久保存，直至重新配置为止，配置完成后通过 AT+RESET 指令重启模块后生效。

1．AT+SSID：网络名称设置命令。注：一定要和路由器的名称对应，20 个字符以内。

例：AT+SSID=TPLINK

返回：<CR><LF>AT+SSID=TPLINK[空格]OK<CR><LF> 配置正确

<CR><LF>AT+SSID=TPLINK[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

2．AT+KEY：网络密码设置命令。注：一定要和路由器密码一致，10 个数字。

例：AT+KEY=0123456789

返回：<CR><LF> AT+KEY=0123456789 [空格]OK<CR><LF> 配置正确

<CR><LF> AT+KEY=0123456789 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

3．AT+BSSID：指定路由器的 BSSID 地址命令。注：如果使用该命令指定路由器地址，一定要和路由器地址完全符合（12 位十六进制码），如果不想指定也可以通过该指令取消指定，

即 AT+BSSID= “”（把 BSSID 地址写入一个空字符串）。

例：AT+BSSID=001EE3A34455

返回：<CR><LF> AT+BSSID=001EE3A34455 [空格]OK<CR><LF> 配置正确

<CR><LF> AT+BSSID=001EE3A34455 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

4．AT+IP：模块 IP 地址设置命令。注：符合标准的 IP 地址格式。

例：AT+IP=192.168.1.110

返回：<CR><LF>AT+IP=192.168.1.110[空格]OK<CR><LF> 配置正确

<CR><LF> AT+IP=192.168.1.110[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

5．AT+NETMASK：模块掩码地址设置命令。注：符合掩码标准格式。

例：AT+NETMASK=255.255.255.0

返回：<CR><LF> AT+NETMASK=255.255.255.0 [空格]OK<CR><LF> 配置正确

<CR><LF> AT+NETMASK=255.255.255.0 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

6．AT+GATEWAY：模块网关地址设置命令。注：与路由器设置一致。

例：AT+GATEWAY=192.168.1.1

返回：<CR><LF>AT+GATEWAY=192.168.1.1[空格]OK<CR><LF> 配置正确

<CR><LF>AT+GATEWAY=192.168.1.1[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

7．AT+DNS：DNS 地址设置命令。注：与路由器设置一致。

例：AT+DNS=192.168.1.1

返回：<CR><LF>AT+DNS=192.168.1.1[空格]OK<CR><LF> 配置正确

<CR><LF>AT+DNS=192.168.1.1[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

8．AT+SERVER：服务器 IP 地址设置命令。注：与服务器 IP 一致。

例：AT+SERVER=192.168.1.10

返回：<CR><LF> AT+SERVER=192.168.1.10 [空格]OK<CR><LF> 配置正确

<CR><LF> AT+SERVER=192.168.1.10 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

9．AT+PORT：服务器端口设置命令。注：与服务器分配的端口一致。

例：AT+PORT=1234

返回：<CR><LF>AT+PORT=1234[空格]OK<CR><LF> 配置正确

<CR><LF>AT+PORT=1234 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

10．AT+CHL：WiFi 信道设置命令。注：与路由器设置一致。

例：AT+CHL=6

返回：<CR><LF> AT+CHL=6 [空格]OK<CR><LF> 配置正确



<CR><LF> AT+CHL=6 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

11．AT+MAC：获取模块 MAC 地址命令。

例：AT+MAC

返回：<CR><LF> AT+MAC[空格]OK<CR><LF>[12 位 MAC 地址]<CR><LF> 操作成功

<CR><LF>ERROR<CR><LF>命令错误

三、GPRS 配置命令

本组命令只能通过 RS232 接口配置，且所有命令配置后永久保存，直至重新配置为止，配置完成后通过 AT+RESET 命令重启模块生效。

1．AT+SERVER：服务器 IP 地址设置。

例：AT+SERVER=122.95.118.15

返回：<CR><LF>AT+SERVER=122.95.118.15 [空格]OK<CR><LF> 配置正确

<CR><LF>AT+SERVER=122.95.118.15 [空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

2．AT+PORT：服务器端口设置命令。

例：AT+PORT=1234

返回：<CR><LF>AT+ PORT =1234[空格]OK<CR><LF> 配置正确

<CR><LF> AT+ PORT =1234[空格]ERROR<CR><LF> 配置错误

<CR><LF>ERROR<CR><LF>命令错误

3．AT+CSQ：GPRS 网络信号查询命令。

例：AT+CSQ

返回：<CR><LF> AT+CSQ[空格]31<CR><LF> 操作正确

<CR><LF>ERROR<CR><LF>命令错误

31 表示信号强度，范围 0～32，数字越大，信号越强，99 表示没有信号。

4．AT+CIMI：CIMI 号查询命令。

例：AT+CIMI

返回：<CR><LF> AT+CIMI [空格]460030916875923 <CR><LF>操作正确

<CR><LF>ERROR<CR><LF>命令错误

460030916875923 为 15 为 CIMI 号。

5．AT+MSM：短信发送命令。

例：AT+MSM=13761226936,MSM Test!

返回：<CR><LF> AT+MSM[空格]OK<CR><LF> 操作成功

<CR><LF> AT+MSM[空格]ERROR<CR><LF> 操作失败

<CR><LF>ERROR<CR><LF>命令错误

注：命令参数由 11 位手机号码和信息内容组成，手机号码与信息内容之间用“,”隔开，信息内容不能只为数字或字符，不支持中文，信息内容长度在 140 个字符以内，超出部分将不



被发送。

系统收到短信后会自动在 RS232 端口打印出信息内容，格式如下：

```
<CR><LF>+CMGR:
"REC UNREAD","+8613761226936","11/07/29,12:06:15+32"<CR><LF>
MSM Test!<CR><LF>
```

说明：+CMGR：短信标识。

"REC UNREAD"：未查阅过的短信。

"+8613761226936"：发送短信的手机号码。

"11/07/29,12:06:15+32"：发送短信的日期时间。

MSM Test!：短信内容。

6．AT+GSMON：GMS 网络启用命令。

例：AT+GSMON

返回：<CR><LF> AT+GSMON[空格]OK<CR><LF> 模块启用成功

<CR><LF> AT+ GSMON [空格]ERROR<CR><LF>模块启用失败

<CR><LF>ERROR<CR><LF>命令错误

7．AT+GSMOFF：GMS 网络禁用命令。

例：AT+GSMOFF

返回：<CR><LF> AT+GSMOFF[空格]OK<CR><LF>模块禁用成功

<CR><LF> AT+ GSMOFF [空格]ERROR<CR><LF>模块禁用失败

<CR><LF>ERROR<CR><LF>命令错误

注：该指令将关闭整个 GPRS 模块电源，GPRS 连接和短信功能禁用。

8．AT+GPRSON：GPRS 网络启用命令。

例：AT+ GPRSON

返回：<CR><LF> AT+ GPRSON[空格]OK<CR><LF>GPRS 功能启用成功

<CR><LF> AT+ GPRSON[空格]ERROR<CR><LF> GPRS 功能启用失败

<CR><LF>ERROR<CR><LF>命令错误

9．AT+GPRSOFF：GPRS 网络停用命令。

例：AT+ GPRSOFF

返回：<CR><LF> AT+ GPRSOFF[空格]OK<CR><LF>GPRS 功能禁用成功

<CR><LF> AT+ GPRSOFF[空格]ERROR<CR><LF>GPRS 功能禁用失败

<CR><LF>ERROR<CR><LF>命令错误

注：该指令只停用 GPRS 连接，GPRS 网络连接禁用，GSM 网络（短信功能）仍可以使用。

四、系统指令

本组命令可以通过 RS232 接口操作，也支持无线通道操作。

1．参数配置命令。命令配置后永久保存，直至重新配置为止。

（1）MMACORRECT(XA,YA,ZA)：加速度传感器数据矫正命令。MMACORRECT 后面由



一个完整的括弧所包含的传感器三个轴向的矫正数据，每个数据由“＋”或“－”符号和两位数值组成，如数值没有十位，则十位用0填充，数据之间以“,”隔开，如果矫正值为＋，则系统会在传感器数据基础上加上相应的值；若矫正值为－，则减去相应的值。

例：MMACORRECT(+20,−04,+00)

返回：<CR><LF>MMACORRECT(+20,−04,+00) [空格]OK<CR><LF>操作成功

<CR><LF>MMACORRECT(+20,−04,+00) [空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（2）STEPMOTSPEED：步进电机转速设置指令。设置范围为30～640转/分钟，此转速为步进电机机芯的转速，电机外轴是电机机芯1/64减速后的转速。

例：STEPMOTSPEED 640（机芯转速640圈/分钟，即外轴10圈/分钟）

返回：<CR><LF> STEPMOTSPEED 600[空格]OK<CR><LF>操作成功

<CR><LF> STEPMOTSPEED 600[空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（3）BELLNULL：取消蜂鸣器报警指令。执行该命令后蜂鸣器不会报警，BELLON指令除外。

例：BELLNULL

返回：<CR><LF>BELLNULL[空格]OK<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

（4）BELLGHGON：蜂鸣器干簧管报警指令。执行该命令后，当干簧管闭合时蜂鸣器立刻报警，直至断开为止。

例：BELLGHGON

返回：<CR><LF>BELLGHGON[空格]OK<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

（5）BELLGASON：蜂鸣器气体传感器报警指令。执行该命令后，当气体传感器TTL电平为低时蜂鸣器立刻报警，直至TTL电平变为高为止。

例：BELLGASON

返回：<CR><LF>BELLGASON [空格]OK<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

（6）BELLBUTTONON：蜂鸣器按键报警指令。执行该命令后，当按键按下时蜂鸣器立刻报警，直至按键抬起为止。

例：BELLBUTTONON

返回：<CR><LF> BELLBUTTONON [空格]OK<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

（7）AT+OVERTIME：网络命令超时设置命令。只用于WiFi和GPRS，设置参数范围为0～9999秒，为0时没有超时检测，当系统检测到超时时，自动重启模块重新连接服务器。

例：AT+OVERTIME=60

返回：<CR><LF> AT+OVERTIME=60 [空格]OK<CR><LF>操作成功

<CR><LF> AT+OVERTIME=60 [空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

2．系统操作指令

（1）DCMOTLEFT：直流电机左向转动指令。

例：DCMOTLEFT

返回：<CR><LF> DCMOTLEFT [空格]OK<CR><LF>操作成功

<CR><LF> DCMOTLEFT [空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（2）DCMOTRIGHT：直流电机右向转动指令。

例：DCMOTRIGHT

返回：<CR><LF> DCMOTRIGHT [空格]OK<CR><LF>操作成功

<CR><LF> DCMOTRIGHT [空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（3）DCMOTSTOP：直流电机右向转动指令。

例：DCMOTSTOP

返回：<CR><LF> DCMOTSTOP [空格]OK<CR><LF>操作成功

<CR><LF> DCMOTSTOP [空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（4）STEPMOTSTEP：步进电机行程设置指令。设置范围（＋/－）0～（＋/－）99999999，此行程是指步进电机机芯所走的步数，电机机芯 64 步/转，电机外轴 4096 步/转，“＋”表示正向转动，“－”表示反向转动。

例：STEPMOTSTEP +4096 （机芯正向转动 64 圈，即外轴正向转动一圈）

返回：<CR><LF> STEPMOTSTEP +4096[空格]OK<CR><LF>操作成功

<CR><LF> STEPMOTSTEP +4096[空格]ERROR<CR><LF>操作失败

<CR><LF>ERROR<CR><LF>命令错误

（5）DSGET：温度传感器 18B20 数据获取指令。

例：DSGET

返回：<CR><LF>DSGET[空格]32.5<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

注：温度值有一位小数位，－5 表示零下 5℃，32.5 表示零上 32.5℃。

（6）SHTGET：温湿度传感器 SHT10 数据获取指令。

例：SHTGET

返回：<CR><LF>SHTGET[空格]32.5[空格]75.5<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

注：返回两组数据中间以空格符隔开，第一组为温度值有一位小数位，－5 表示零下 5℃，32.5 表示零上 32.5℃；第二组数据为湿度，为百分比数值，比如返回 75.5 则表示当前湿度为 75.5%。

（7）MMAGET：加速度传感器数据获取指令。

例：MMAGET



返回：<CR><LF>MMAGET[空格]X:21[空格]Y:42[空格]Z:-35<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

注：返回三组数据分别为 X，Y，Z 三轴方向的加速度值，中间由空格符隔开，计算单位为 2g/64，g 通常为 9.8，每个轴的量程为－2g～＋2g，对应数值为－64～＋64。

（8）BUTTONGET：按键状态获取指令。

例：BUTTONGET

返回：<CR><LF> BUTTONGET [空格]DOWN <CR><LF>操作成功
<CR><LF> BUTTONGET [空格]UP <CR><LF>操作成功
<CR><LF> ERROR <CR><LF>操作失败

（9）GASCO2GET：气体传感器数据获取指令。

例：GASCO2GET

返回：<CR><LF> GASCO2GET [空格]300[空格]HIGH<CR><LF>操作成功
<CR><LF> ERROR <CR><LF>命令错误

注：第一个数据为气体浓度表示值，则表示浓度值，300～35000ppM；后面一个值为 TTL 电平状态，LOW 表示低电平，HIGH 表示高电平。

（10）GASMQ2GET：MQ2 气体传感器数据获取指令。

例：GASMQ2GET

返回：<CR><LF> GASMQ2GET [空格]4500[空格]HIGH<CR><LF>操作成功
<CR><LF> ERROR <CR><LF>命令错误

注：第一个数据为气体传感器输出模拟信号电压值，单位为毫伏，电压越高浓度越大，后面一个值为 TTL 电平状态，LOW 表示低电平，HIGH 表示高电平。

（11）GASMQ5GET：MQ5 气体传感器数据获取指令。

例：GASMQ5GET

返回：<CR><LF> GASMQ5GET [空格]4500[空格]HIGH<CR><LF>操作成功
<CR><LF> ERROR <CR><LF>命令错误

注：第一个数据为气体传感器输出模拟信号电压值，单位为毫伏，电压越高浓度越大，后面一个值为 TTL 电平状态，LOW 表示低电平，HIGH 表示高电平。

（12）GASLSGET：光敏传感器模块数据获取指令。

例：GASLSGET

返回：<CR><LF> GASLSGET [空格]50[空格]HIGH<CR><LF>操作成功
<CR><LF> ERROR <CR><LF>命令错误

注：第一个数据为光强度百分比，50 表示 50%，后面一个数据为模块 TTL 电平状态，LOW 表示低电平，HIGH 表示高电平。

（13）LSGET：板载光敏电阻数据获取指令。

例：LSGET

返回：<CR><LF>LSGET[空格]50<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

注：返回数值为光强度百分值，50 表示强度 50%。

（14）GHGGET：干簧管/按键状态获取指令。

例：GHGGET

返回：<CR><LF>GHGGET[空格]OFF<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

注：返回 OFF 表示断开或按键抬起，返回 CLOSE 表示连接或按键按下。

（15）IRGET：人体感应传感器状态获取指令。

例：IRGET

返回：<CR><LF>IRGET[空格]HIGH<CR><LF>操作成功

<CR><LF>ERROR<CR><LF>命令错误

注：返回 HIGH 表示高电平，已触发；返回 LOW 表示低电平，未被触发。

（16）VBATGET：电池电压获取指令。

例：VBATGET

返回：<CR><LF>VBATGET[空格]4.995<CR><LF>操作成功

<CR><LF>ERROR <CR><LF>命令错误

注：返回数据带 3 位小数，单位为 V。

（17）VSYSGET：系统 5V 电源电压获取指令。

例：VSYSGET

返回：<CR><LF> VSYSGET [空格]4.995<CR><LF>操作成功

<CR><LF>ERROR <CR><LF>命令错误

注：返回数据带 3 位小数，单位为 V。

（18）ALLGET：一次性获取所有数据指令。返回以 AA 55 开头的 35 个十六进制数据。

例：ALLGET

返回：AA 55 20 FF FF 00 00 40 00 4A 01 58 01 9E 02 92 01 85 13 57 13 64 00 2A 01 00 00 00 00 C0 01 0B 18 FC 86 操作成功，数据解析如表 B-1 所示。

<CR><LF> ERROR <CR><LF>命令错误

表 B-1 数据解析结果

包头		数据长度	X 轴低位	X 轴高位	Y 轴低位	Y 轴高位	Z 轴低位	Z 轴高位	18B20 低位	18B20 高位	SHT 温度低位	SHT 温度高位	SHT 湿度低位
Byte1	Byte 2	Byte 3	Byte4	Byte 5	Byte 6	Byte7	Byte8	Byte 9	Byte10	Byte11	Byte12	Byte13	Byte14
SHT 湿度高位	GAS 低位	GAS 高位	输入电压低位	输入电压高位	5V 电压低位	5V 电压高位	电机转速低位	电机转速高位	板载光敏强度	蜂鸣器状态	电机状态	LED 灯	数码管 1
Byte15	Byte16	Byte17	Byte18	Byte19	Byte 20	Byte21	Byte22	Byte23	Byte24	Byte25	Byte26	Byte27	Byte28
数码管 2	TTL 电平信号	GAS 状态	X 轴矫正值	Y 轴矫正值	Z 轴矫正值	超时低位	超时高位	GSM 状态	GPRS 状态	预留	预留	预留	校验和
Byte29	Byte30	Byte31	Byte32	Byte33	Byte34	Byte35	Byte36	Byte37	Byte38	Byte39	Byte40	Byte41	Byte42

固定包头为：0xAA，0x55。



数据长度为：0x20，不包含包头和本身。

X 数据：16 位整型带符号。

Y 数据：16 位整型带符号。

Z 数据：16 位整型带符号。

18B20 数据：16 位符号整型，注意符号位，包含一位小数，如 325 表示 35.2℃。

SHT 温度：同 18B20 数据。

SHT 湿度：16 位整型，包含一位小数，755 表示 75.5%。

GAS 数据：16 位整型，没有小数。

输入电压：16 位整型，三位小数，单位 V。

5V 电压：同输入电压。

电机转速：16 位整型，30～640，详见 MOT2SPEED 命令。

板载光敏强度：8 位，0～100%。

蜂鸣器状态：8 位，bit8：1 表示蜂鸣器正在鸣叫，0 表示没有鸣叫。

bit0～bit6：0 表示蜂鸣器不受任何输入信号影响。

1 表示干簧管闭合，蜂鸣器鸣叫，断开停止鸣叫。

2 表示气体传感器 TTL 电平为低时鸣叫，为高时停止鸣叫。

电机状态：8 位，bit0～bit3：0 表示直流电机停止，1 表示右转，2 表示左转。

bit4～bit7：0 表示步进电机停止，1 表示步进电机右转，2 表示步进电机左转。

LED 灯：8 位，LED 灯目前的状态，bit0～bit3 对应板载 LED5～LED8，bit4～bit7 对应 LED 模块 LED1～LED4，0 表示亮，1 表示灭。

数码管 1：8 位，第一位数码管显示状态，详见 LED2SET 命令。

数码管 2：8 位，第二位数码管显示状态，详见 LED2SET 命令。

TTL 电平信号：8 位，bit7：干簧管 TTL 电平。

bit6：气体传感器 TTL 电平。

bit5：人体感应传感器 TTL 电平。

GAS 状态：8 位，1 表示 CO_2 传感器，2 表示 MQ2 传感器，3 表示 MQ5，4 表示光敏传感器。

X 轴矫正值：8 位，带符号型。

Y 轴矫正值：8 位，带符号型。

Z 轴矫正值：8 位，带符号型。

超时：16 位，0～9999 秒，0 表示没有超时检测（超过该设定时间未收到服务器任何操作命令或数据，则认为系统与服务器连接异常，系统自动重新连接服务器）。

GSM 状态：0 表示禁止，1 表示启用；当 GSM 禁止时，GPRS 模块电源处于关闭状态，基于 GPRS 模块的所有功能均不能使用。

GPRS 状态：0 表示禁止，1 表示启用；当 GPRS 网络被禁用时，系统不能通过 GPRS 连接到服务器，但 GSM 网络功能仍可以用，即短信功能可以正常使用。

校验和：8 位，所有数据字节（不包括包头和包长度字节及校验和本身）相加，取低 8 位。

（19）RELAY1OUT：继电器 1 输出指令。

例：RELAY1OUT

返回：<CR><LF>RELAY1OUT[空格]OK<CR><LF>操作成功

（20）RELAY1OFF：继电器 1 关闭指令。

例：RELAY1OFF

返回：<CR><LF>RELAY1OFF[空格]OFF<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

（21）RELAY2OUT：继电器 2 输出指令。

例：RELAY2OUT

返回：<CR><LF>RELAY2OUT[空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

（22）RELAY2OFF：继电器 2 关闭指令。

例：RELAY2OFF

返回：<CR><LF>RELAY2OFF[空格]OFF<CR><LF>操作成功
<CR><LF>ERROR <CR><LF>命令错误

（23）LED1SET[Hex]：LED 灯操作指令。LED1SET 后面加一个 8 位的十六进制数，8 位分别表示 8 个 LED 灯的状态，对应位为 0 表示亮，1 表示灭。bit0～bit3 对应板载 LED5～LED8，bit4～bit7 对应模块 LED1～LED4。

例：LED1SET[0xEE] （板载 LED5 亮，模块 LED1 亮，其他灯灭）

返回：<CR><LF>LED1SET[0xEE][空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

（24）LED2SET[Hex][Hex]：数码管操作指令。LED2SET 后面加两个 8 位的十六进制数，8 位分别表示每个数码管的 8 段码的状态，对应位为 0 表示亮，1 表示灭。bit0～bit7 对应数码管 a，b，c，d，e，f，g，dp。

例：LED2SET[0xC0][0xF9] （数码管第一位显示 0，第二位显示 1）

返回：<CR><LF>LED2SET[0xEE][0XF9][空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

（25）BELLON：蜂鸣器鸣叫命令。

例：BELLON

返回：<CR><LF>BELLON [空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

注：蜂鸣器鸣叫时，响 0.5 秒，停 0.5 秒。

（26）BELLOFF：蜂鸣器关闭命令。

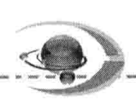
例：BELLOFF

返回：<CR><LF>BELLOFF[空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误

（27）AT+RESET：模块重启命令。系统接收到该命令后自动重新启动模块。

例：AT+RESET

返回：<CR><LF> AT+RESET[空格]OK<CR><LF>操作成功
<CR><LF>ERROR<CR><LF>命令错误



五、GPRS 版本二次开发注意事项

1．由于 GPRS 模块、GSM 网络、GPRS 网络的特殊性，所以在二次开发过程中应特别注意。

2．GPRS 模块初始化过程中参数配置比较繁杂，所以每次初始化时间比较长，在移动网络正常情况下，本地卡初始化时间为 1～1.5 分钟，漫游卡初始化时间为 1～2 分钟。

3．系统在 GPRS 模块初始化过程不接受 RS232 接口的所有命令及数据操作，待模块初始化结束后再对所受到的命令进行回复处理，所以使用者在二次开发过程中应该特别注意这一点。

4．系统上电后会对 GPRS 模块进行初始化，同时 RS232 接口输出<CR><LF>GSM STARTING!<CR><LF>字符输出，配置时间一般为 10 秒～2 分钟，初始化结束后 RS232 接口输出<CR><LF>GSM OK!<CR><LF>或<CR><LF>GSM ERROR!<CR><LF>字符串，表明初始化成功或失败；如果模块初始化失败系统会在 30 秒后尝试重新初始化模块，直到初始化成功或接收到 AT+GSMOFF 命令为止。如果 GPRS 模块初始化成功，随后系统会对 GPRS 网络进行配置，系统会根据存储器里保存的服务器信息进行连接，配置时间一般为 10 秒～2 分钟，视网络情况及服务器运行情况而定，连接完成后 RS232 接口输出<CR><LF>GPRS OK!<CR><LF>或<CR><LF>GPRS ERROR!<CR><LF>；若连接失败，系统会在 20 秒钟后尝试重新连接，若连续 3 次连接不成功，系统自动重新初始化 GPRS 模块，再进行下一次连接，直至 GPRS 连接成功或收到 AT+GPRSOFF 为止。当系统在正常运行中，出现需要重新初始化 GPRS 模块时，RS232 接口输出<CR><LF>GSM RESTARTING!<CR><LF>，待初始化完成后，RS232 接口输出<CR><LF>GSM OK!<CR><LF>或<CR><LF>GSM ERROR!<CR><LF>表示连接成功或失败；系统正常运行中对 GPRS 网络连接进行重新配置后，RS232 接口输出<CR><LF>GPRS OK!<CR><LF>或<CR><LF>GPRS ERROR!<CR><LF>表示配置成功或失败。

5．当出现系统异常、网络异常、配置参数不正确导致系统长时间处于模块初始化或 GPRS 网络配置中，此时可以通过 AT+GSMOFF 指令或 AT+GPRSOFF 指令停用 GPRS 模块或停用 GPRS 网络连接，停用后系统会在最短时间内退出模块重复初始化或重复连接 GPRS 网络状态，此时可以进行正常系统参数配置，配置完成后再使用 AT+GSMON 或 AT+GPRSON 指令启用 GSM 模块或 GPRS 网络连接。详情参考指令说明。

6．所有系统参数和状态都可以通过 ALLGET 指令查询，详情见 ALLGET 指令详解。

参 考 文 献

[1] 王志良．物联网现在与未来．北京：机械工业出版社，2010.

[2] 张福生．物联网开启全新生活的智能时代．太原：山西人民出版社，2010.

[3] 周洪波．物联网技术、应用、标准和商业模式．北京：电子工业出版社，2010.

[4] 陈柳钦．物联网：国内外发展动态及亟待解决的关键问题．[2010-08-11]．价值中国网．

[5] 张云霞．物联网商业模式探讨．电信科学，2010（4）.

[6] 宁焕生，王炳辉．RFID 重大工程与国家物联网．北京：机械工业出版社，2009.

[7] 项有建．冲出数字化．北京：机械工业出版社，2010.

[8] 吴功宜．智慧的物联网．北京：机械工业出版社，2010.

[9] 移动支付——悄然兴起．北京青年报，2003-01-07.

[10] 郑海初．正在爆发的物联网革命．北京：中华工商联合出版社，2010.

[11] 宁焕生，张彦．RFID 与物联网——射频、中间件、解析与服务．北京：电子工业出版社，2010.

[12] 余立建，王茜，李文仲．物联网/无线传感网实践与实验．西安：西安交通大学出版社，2010.

[13] 语音识别．维基百科．

[14] 刘云浩．物联网导论．北京：科学出版社，2010.

[15] 郭雷勇．RFID 系统的防冲突算法研究与实现．中山大学博士学位论文，2009.11.

[16] 张飞舟，杨东凯，陈智．物联网技术导论．北京：电子工业出版社，2010.

[17] 厂商识别代码索引编码的 64 位标签转化为 EAN UCC 厂商识别代码．

[18] 马建．物联网技术概论．北京：机械工业出版社，2011.

[19] 张鸿涛，徐连明，张一文．物联网关键技术及系统应用．北京：机械工业出版社，2012.

[20] 周洪波．物联网技术、应用、标准和商业模式．北京：电子工业出版社，2011.

[21] 康东．射频识别（RFID）核心技术与典型应用开发案例．北京：人民邮电出版社，2008.

[22] 黄林国，娄淑敏，谢杰．计算机网络技术项目化教程．北京：人民邮电出版社，2011.

[23] 张成海，张铎．物联网与产品电子代码（EPC）．北京：武汉大学出版社，2010.

[24] 陈滢．浅析 RFID 在现代零售业中的应用．江苏商论，2008（4）.

[25] 任丰原，黄海宁，林闯．无线传感器网络．软件学报，2005，14（7）：1282-1291.

[26] 孔晓波．物联网概念和演进路径．电信工程技术与标准化，2009，9（12）：18-29.

[27] 施鹏，赵华伟．ZigBee 传感网的一种新型安全方案．计算机系统应用，2011，Vol.20（8）：204-207.

[28] 宋合营，赵会群．物联网分布式识读器数据采集方案设计与实现．北方工业大学学报，2008，2（1）：66-68.

[29] 侯雷．无线传感器网络及相关问题研究．计算机安全，2010，7：46-50.



[30] 刘涛．无线传感器网络安全的优化研究，计算机仿真，2011，28（7）：158-160，219．

[31] 宋和平，胡成全，樊东霞等．基于簇的无线传感器网络密钥管理方案．吉林大学学报（信息科学版），2011，29（3）：231-236．

[32] 余旺科，马文平，陈和风．分簇无线传感器网络密钥管理方案．西南交通大学学报，2011，46（2）：310-314．

[33] 颜珍平，颜谦和．无线传感器网络密钥分配方法研究，计算机仿真，2011，28（4）：133-136．

[34] 孔繁瑞，李春文．无线传感器网络动态密钥管理方法．软件学报，2010，21（7）：1679-1691．

[35] 杜志强，沈玉龙，马建峰．基于信息覆盖的无线传感器网络访问控制机制．通信学报，2010，31（2）：113-118．

[36] 何伟刚．物联网中 RFID 节点通信安全研究．信息安全与技术，2011（7）：21-24．

[37] 高磊，盛焕烨．RFID 应用系统中 Tag-reader 安全通信协议．计算机工程，2007，Vol.33（21）：128-130．

[38] 李静，夏幼明，姜懿庭．Gen2 标签的 RFID 认证协议的研究．云南民族大学学报（自然科学版），2010，Vol．19（4）：241-244．

[39] 胡国胜．RFID 系统安全分析．计算机安全，2013（1）：67-71．

[40] A. Koelle, S. Depp, and R. Freyman, “Short-range radio-telemetry for electronic identification, using modulated RF backscatter.” Name: Proc. IEEE, 1975.

[41] ITU Internet Reports 2005：The Internet of Things- Executive Summary.

[42] R.F.Harrington, “Theory of loaded scatters” Elesrical Engineers, Proceedings of the Institution of, Vol 111, pp. 617-623, 1964.